Al-Azhar University

Faculty of Engineering

Electrical Engineering Department

B.Sc.

GRADUATION PROJECT

Smart Enterprise Network Architecture

Supervised by :

Dr Ahmed Zakzouk **Dr Ragab Elsagher**

PRESENTED BY:

Esraa Mohamed Hegazy	ID :20265102
Hager Ramadan Soliman	ID :20265199
Nouran Taher Ali	ID :20265194
Mona Muhammad Elsayed	ID :20265189
Nehal Hany Basha	ID :20265192

July2026

CamScanner

Acknowledgement

First and foremost we would like to praise our creator Allah the Almighty, the most Gracious and the most Merciful for his blessing given to us during our study and in completing this project.

We would like to express our heartfelt gratitude to our supervisor, **Dr Ahmed Zakzouk**, for the continuous support of our graduation project and research; I would happily express my warm and deep thanks to him also for his constructive and detailed comments, and for his mandatory support throughout this work.

Also, we cannot forget our college **Faculty of Engineering Al-Azhar University** forgiving us a good education, help and chances to achieve our goals.

Finally, we will never find enough words to express the gratitude and appreciation that we owe to our families for their constant support, encouragement, never- ending patience as well as their love that raised us up again when we got weary and without them, we doubt that we would be in this place today.

CamScanner

Chapter1: Computer Network

1. 1 Computer network work

Network is group of component that connected together to provide a specific services like exchange data and resources, shares files with each other. A network connection between these devices can be established by using cables or wireless media.

Intermediate devices interconnect end devices. Such as switches, wireless Access points, routers, and firewalls Management of data through a network.

The intermediate devices (network devices) contains basic devices like switch, router, modem and NIC (network interface card), and contains advanced devices such as firewall, IDS (instruction detection system),IPS (instruction prevention system) and wireless access point .using advanced intermediate devices or basic according to the size of network and the services that have been applied.

An end device is where a message originates from or where it is received or transmitted. [1]

1.2 Computer network design

1.2.1 Hierarchical design

Contains: switch core, designated and access

CamScanner

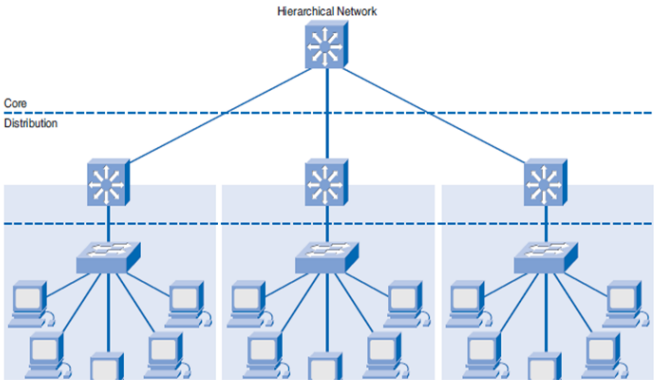


Figure 1.1 hierarchical design

1.2.2Collapsed core

Network contains Core switch or distribution switch in the same layer and access switch in another layer.

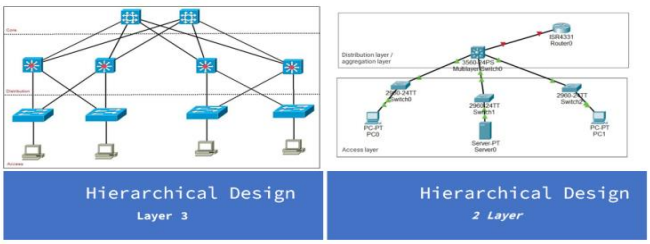


Figure 1.2 Collapsed core

1.3 Computer network types

1.3.1 Local area networks (LANs)

The group of devices that connect together in the small area (small geographic area), such as building floor, a building or adjacent buildings this is called local area network **(LAN).** The advantage of a LAN is that all network elements are close together.

CamScanner

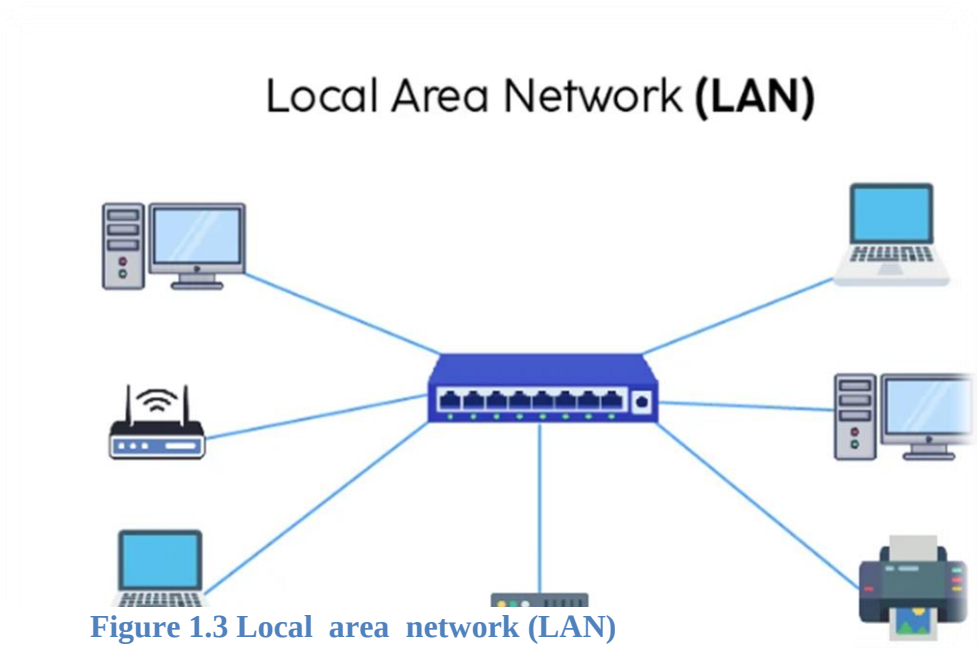


Figure 1.3 Local area network (LAN)

LAN characteristics

- Short distance (max is 100m)
- High speed
- Low cost
- Ease of access

1.3.2 Wide area networks (WANs)

It is group of LANS connected in the wide area network (over wide geographic area. the technology that connects your offices, data centers, cloud applications, and cloud storage together. It is called a wide-area network because it spans beyond a single building or large campus to include multiple locations spread across a specific geographic area, or even the world .some advantages of a wan the communication over long distance , **the biggest WAN is Internet (public WAN).**

CamScanner

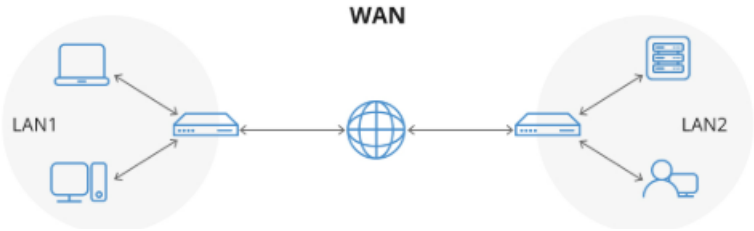


Figure 1.4 WAN topology

1.3.3 Metropolitan area network (MAN)

A metropolitan area network **(MAN)** is a computer network that connects computers in a metropolitan area which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN). [2]

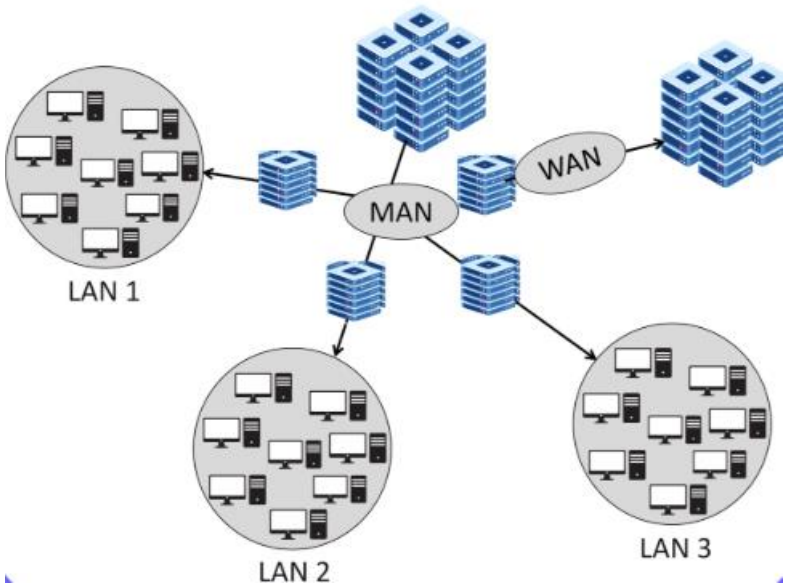


Figure 1.5 MAN topology

1.4 Network Topology

The network topology explains how devices connected together over LAN, WAN or MAN.

CamScanner

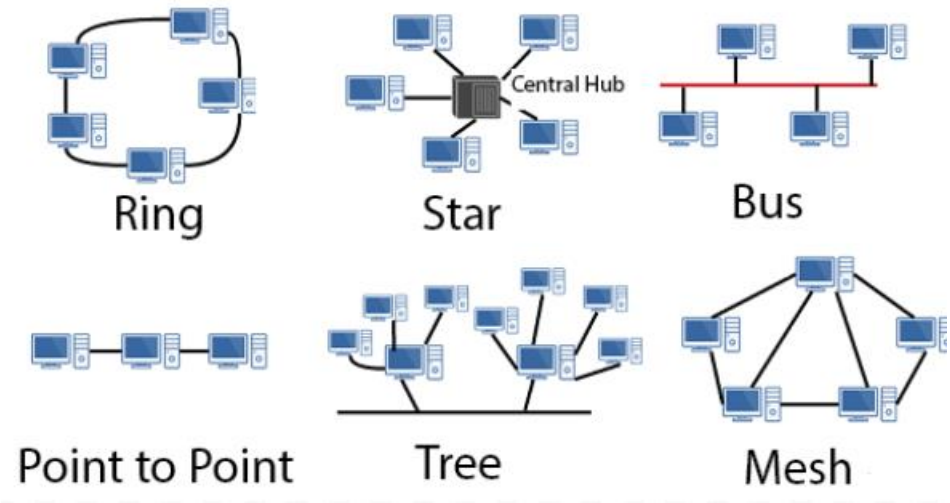


Figure 1.6 Network topology

1.4.1point to point (p2p)

Point to point connection, is a network topology where two nodes are connected directly to each other without any intermediate device

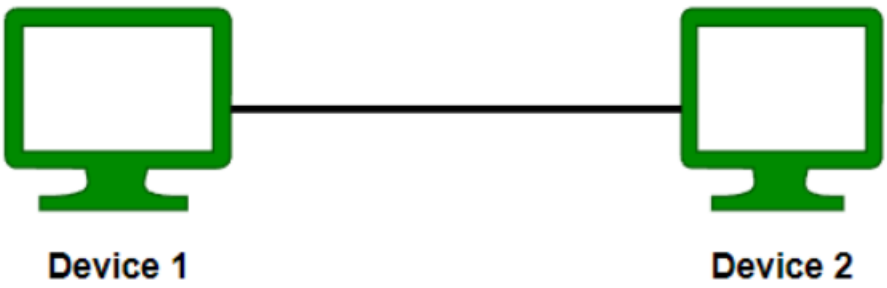


Figure 1.7 Point to point topology

CamScanner

1.4.2 Bus topology

Bus topology is a network topology where all network devices are connected to a single shared communication medium and single collision domain, typically coaxial cable or a twisted pair cable .The probability of collision.

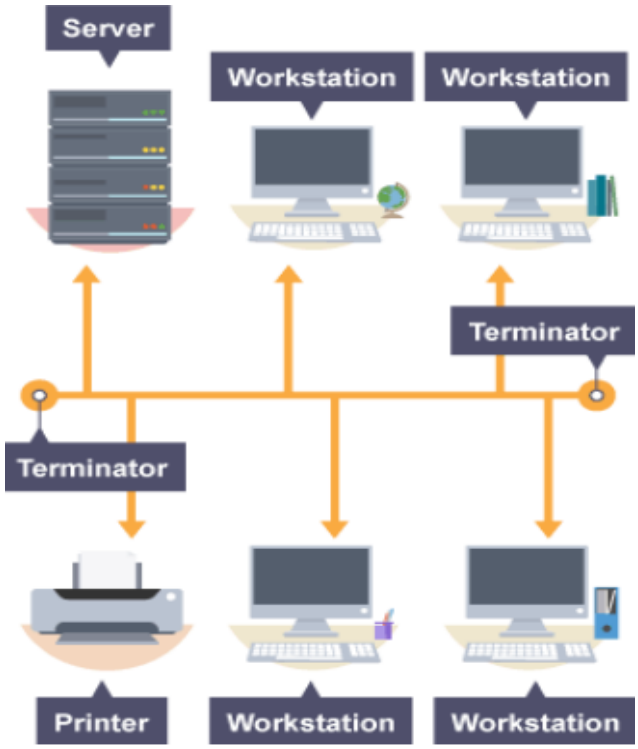


Figure 1.8 Bus topology

1.4.3 Ring topology

The ring topology is a network topology where the network devices connected in the circular fashion forming a closed loop, each device in the ring topology connected with two devices creating a continuous path ,this type of connection need more one NIC over one device and the same foe the cables.

CamScanner

Figure 1.9 Ring topology

1.4.4 Mesh topology

Mesh topology is a network topology where each node is connected with all network devices .There are a multiple paths available for transmitting data, that creating high redundancy.

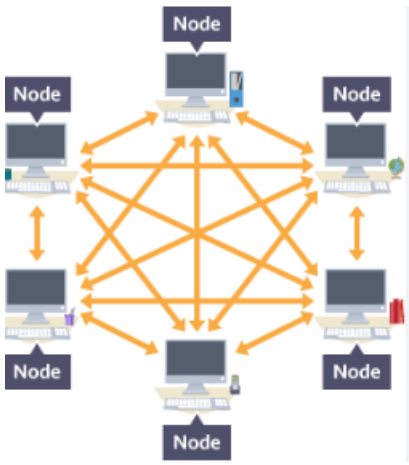


Figure 1.10 mesh topology

CamScanner

1.4.5 Star topology

Star topology is a network setup where each device connects to a central hub or switch .The communication between the devices is simple with less collision and less NIC.

This design resembles a star, with cables radiating from the hub, allowing for efficient communication and management of network traffic. Star topology is widely used in homes, offices and schools due to its reliability and the ease with which devices can be added or removed easily. [3]

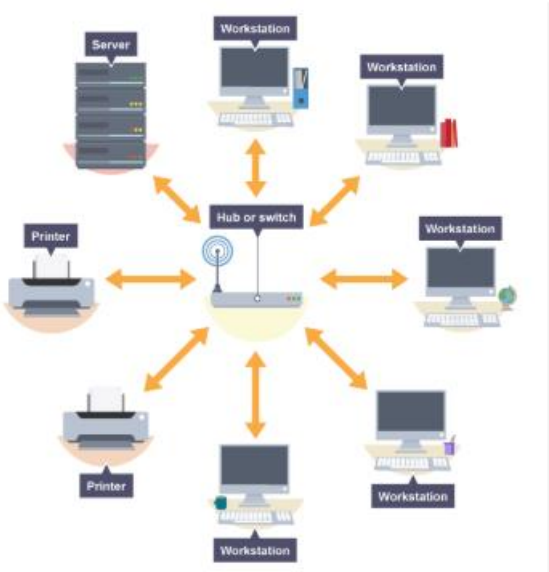


Figure 1.11 Star topology

1.5 Network Model

1.5.1 Open system interconnection (OSI)

The OSI (Open Systems Interconnection) model is a conceptual framework that describes how networked systems communicate. It's a standardized way to understand and

CamScanner

organize network communication by breaking it down into seven distinct layers. Each layer has specific responsibilities, and data flows between them, encapsulating and transmitting data in a structured manner.

Each of the seven layers performs a specific function and communicates with the layer above and below it. Today OSI model is primarily used as a reference model to explain how the device has been communicated.

The OSI model distinguished in seven abstraction layers: physical layer, datalink layer, network layer, transport layer, session layer, presentation layer and application layer.

OSI model provides a blueprint for understanding and building complex network systems, making it easier to design, manage, troubleshoot, and innovate in the world of networking.

The OSI model provides a common language and framework for understanding how networks function, allowing engineers to visualize and discuss network behavior in a structured way.

By dividing network communication into layers, the OSI model allows for focused development, troubleshooting, and updates on specific layers without affecting the entire system.

CamScanner

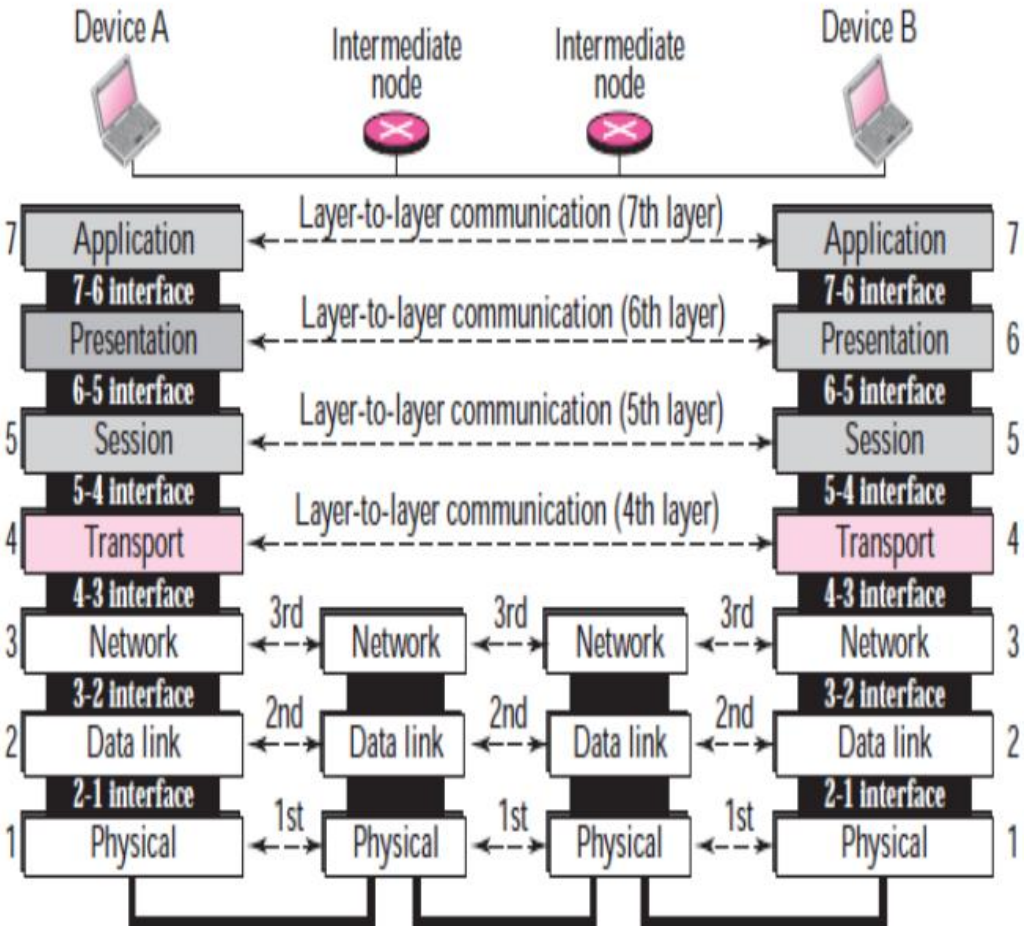


Figure 1.12 open system interconnection (OSI)

1.5.1.1 Application layer

It is the interface of the network in front of user, it is responsible for preparing the initial request or reply for prepare a service, this layer contains important protocols:

- **Telnet:** Remote login.
- **HTTP:** (hypertext transfer protocol) allow to access data over the world wide web , it is transfer data with plain text it is the disadvantages , so it is recommended to use **HTTPs** transfer data encrypted.
- **FTP** (file text protocol): Transmit and receive the files.
- **POP (**post office protocol): Receive mails.

CamScanner

- **SMTP** (simple mail transfer protocol): Sending mails.

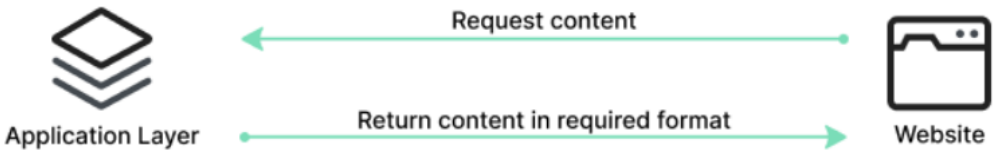


Figure 1.13Application layer

- **DNS** (domain name system): It has been used to resolve domain name over the IP address to make the communication simple. People prefer to connect with name instead of addresses.

1.5.1.2 Presentation layer

The presentation layer, often called the (syntax layer) or (translation layer), It acts as a translator, converting data between the application layer and the network format, ensuring data is presented in a readable format for the receiving application. This layer handles tasks such as data formatting, encryption/decryption and it is responsible for adding the suitable extension for the data.

Figure 1.14 Presentation layer

1.5.1.3 Session layer

The Session Layer is integral to network communication, ensuring that data exchanges are reliable and

CamScanner

efficient. It manages the initiation, maintenance, and termination of communication sessions, which is essential for seamless data transfer.

The basic and most important function of the session layer is to establish a connection between the communicating parties known as sessions. This connection helps to transfer the data such as files, remote login, and communication over these sessions in a more ordered and reliable way.

The layer sets up a session by coordinating and negotiating parameters, such as protocols and port numbers, to ensure compatibility between devices (Establishing Sessions), session management and session treatment.

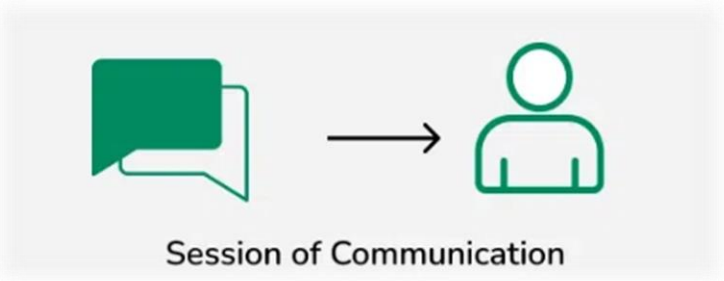


Figure 1.15 session layer

1.5.1.4 Transport layer

The transport layer, also known as Layer 4 in the OSI model, is responsible for end-to-end communication between applications, ensuring reliable and efficient data delivery. It handles tasks like segmentation, reassembly, flow control, and error control.

Transport layer divide data into small parts called **data part** and attached the source and destination part this called

CamScanner

segment, this process called segmentation .This layer has two software TCP and UDP.

Figure 1.16 transport layer

The transport layer has two software T CP, UDP. TCP and UDP are both transport layer protocols in computer networking, but they differ significantly in how they handle data transmission. TCP (Transmission Control Protocol) is connection-oriented, reliable, and ordered, making it suitable for applications requiring data integrity. UDP (User Datagram Protocol) is connectionless, faster, and less reliable, ideal for applications where speed is paramount, even if some data loss is acceptable.

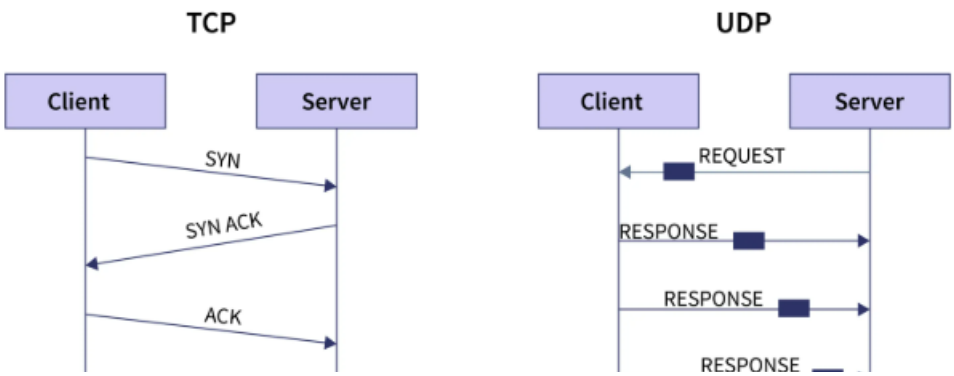


Figure 1.17 TCP&UDP

1.5.1.5 Network layer

The network layer, also known as Layer 3 in the OSI model, is responsible for routing and forwarding data packets

CamScanner

between different networks. It handles the logical addressing (like IP addresses) and determines the best path for data to travel from source to destination. Essentially, it connects networks and enables communication between devices on different networks.

Network layer attached the segment with the destination and source IP address the result called **packet**.

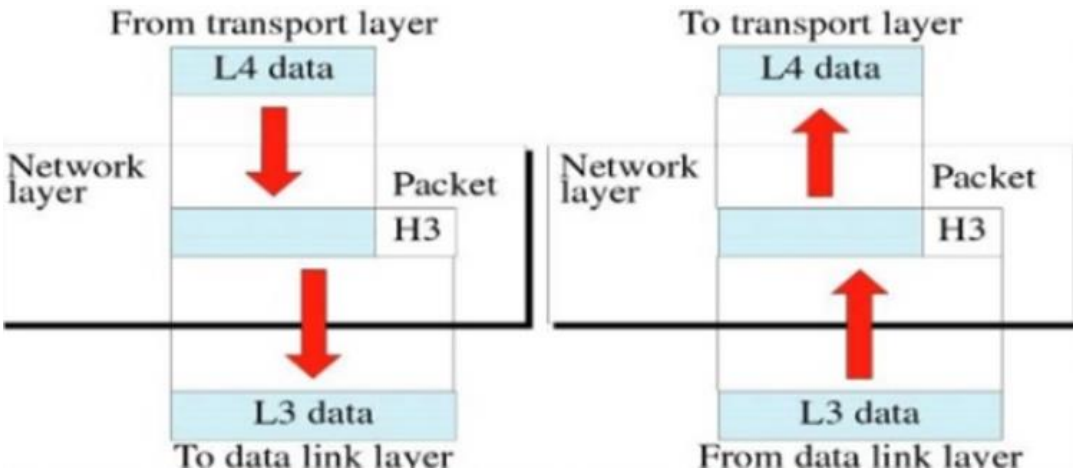


Figure 1.18Network layer

1.5.1.6 Data link layer

The data link layer, also known as Layer 2 in the OSI model, is responsible for reliable data transfer between two directly connected nodes on a network. It handles the physical addressing, error detection, flow control, and manages access to the physical medium. Essentially, it ensures data packets are framed, transmitted, and received correctly between devices on the same network segment.

The data link layer attached the packet with source mac and destination mac the result is **frame.**

CamScanner

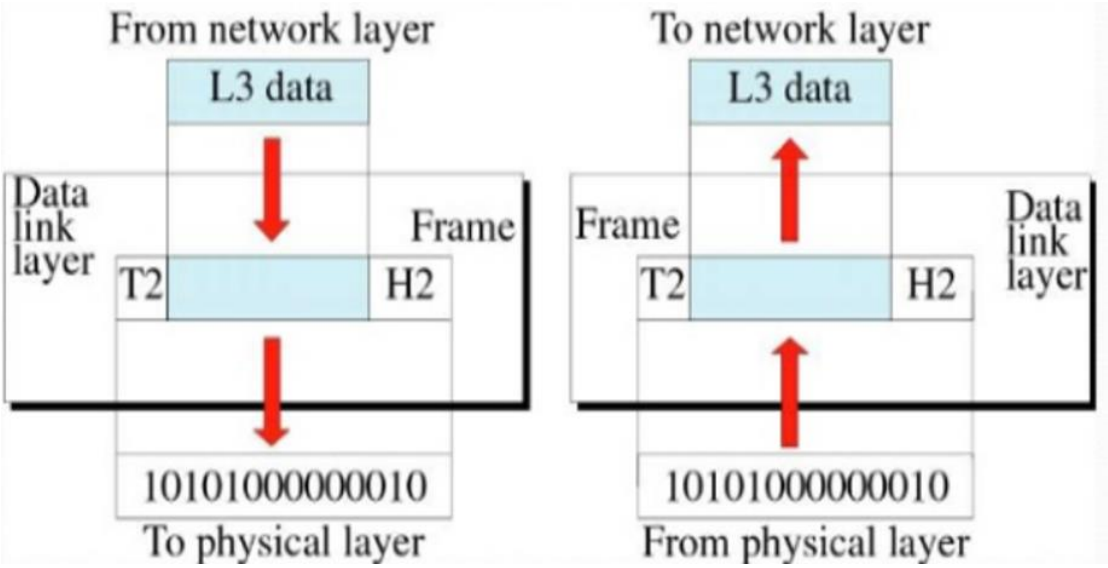


Figure 1.19 data link layer

1.5.1.7 Physical layer

The physical layer is the first and lowest layer of the OSI model, responsible for the physical transmission of data over a network medium. It defines the electrical, mechanical, and functional specifications for transmitting bits (ones and zeros) over a physical connection, such as cables or wireless signals. Essentially, it's the layer that gets the data from one device to another, physically. [4]

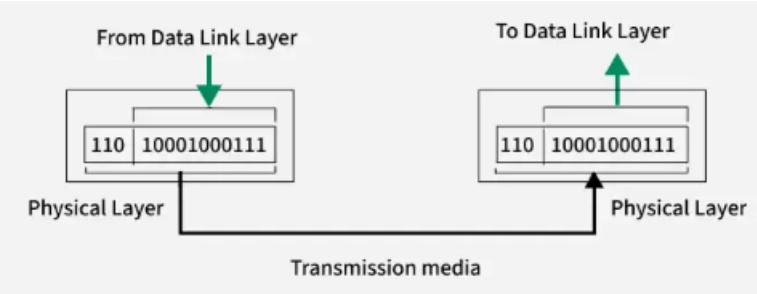


Figure 1.20 Physical layer

CamScanner

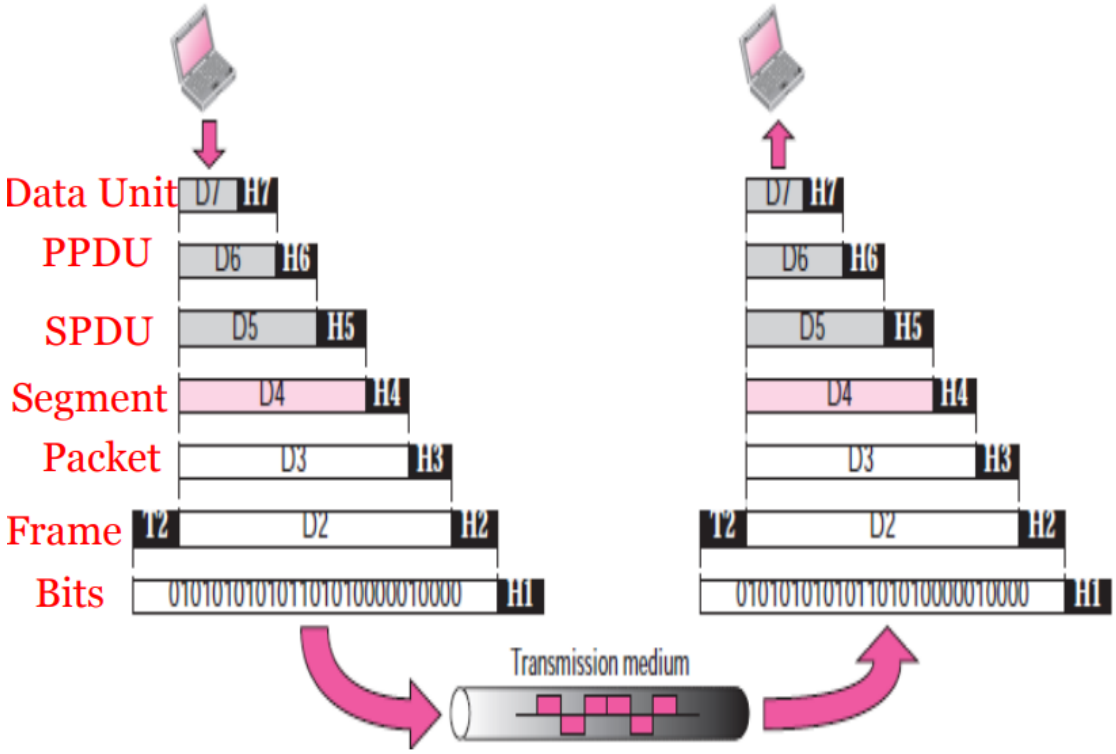


Figure 1.21 OSI process

1.5.2 TCP/IP

The TCP/IP model, also known as the Internet protocol suite, is a framework that standardizes how data is transmitted over networks. It's a four-layer model, consisting of the Link, Internet, Transport, and Application layers, each handling specific aspects of communication. This model ensures interoperability between different devices and networks by defining how data should be formatted, addressed, transmitted, routed, and received.

CamScanner

TCP/IP originated in the 1970s when two Defense Advanced Research Projects Agency (DARPA) scientists, Vinton Cerf and Bob Kahn, created it. It was initially the standard protocol for the Advanced Research Projects Agency Network (ARPANET) and is sometimes called the internet protocol suite.

TCP/IP is the core set of protocols that define how data is transmitted and received over the internet.

TCP ensures that data packets are delivered reliably, even across large distances, by handling things like error checking and retransmitting lost packets. TCP/IP is the foundation for many modern technologies, including cloud computing, IoT, and mobile technologies.

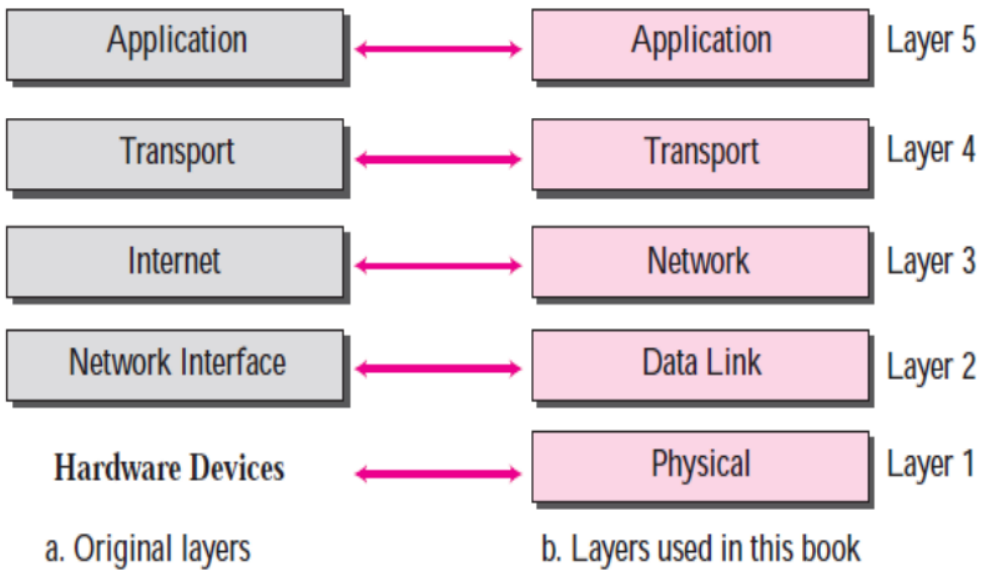


Figure 1.22 OSI&TCP

1.6 Network devices

Network devices are crucial for establishing and maintaining communication pathways, ensuring data is

CamScanner

transmitted and received securely and efficiently. They enable connectivity, manage traffic flow, provide security features, and facilitate resource sharing within a network and with the internet. Without these devices, seamless communication, efficient data transfer, and robust security measures would be impossible, impacting both personal and business operations.

1.6.1 Hub

In networking, a hub is a simple network device that connects multiple devices together in a Local Area Network (LAN). It operates at the physical layer (Layer 1) of the OSI model, meaning it receives data packets and broadcasts them to all connected devices, regardless of the intended recipient. Essentially, a hub acts as a common connection point, but it lacks the intelligence to direct traffic efficiently.

Hub has some types, using hub in the network is not recommended

Figure 1.23 HUB

CamScanner

1.6.1 .1 Active hub

The device that connects multiple devices and also regenerates and amplifies incoming data signals before retransmitting them to other connected devices. This regeneration capability helps overcome signal degradation over longer distances and allows for a larger number of connected devices. Active hubs are also sometimes referred to as (multiport repeaters).

Figure 1.24 active hub

1.6.1.2 Passive hub

A passive hub in a computer network acts as a simple connection point, passively relaying data signals between devices without any processing or amplification. Unlike active hubs, they don't require a power source and are primarily used for basic connectivity in small networks.

1.6.1 .3Intelligent hub

An intelligent hub in a network is a network device that combines the basic functionality of a hub with additional features like monitoring, management, and troubleshooting

CamScanner

capabilities. It acts as a central connection point for multiple devices and can analyze network traffic, detect issues, and even isolate problematic devices.

1.6.2Repeater

Repeater is a type of network node that amplifies incoming signals and rebroadcasts them over a wider area or higher network layer than the original signal. In computer networks, a repeater is used to increase the network's reach, restore a damaged or weak signal, or provide access to inaccessible nodes.

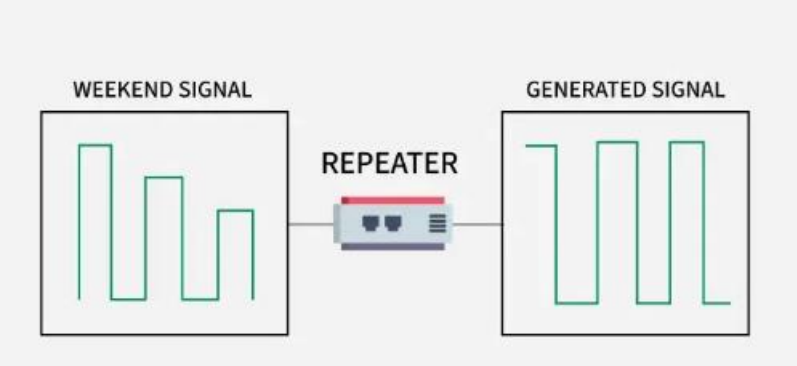


Figure 1.25Repeater

CamScanner

1.6.3Bridge

A bridge is a network device that connects multiple subnetworks to create a single network. It provides interconnection with other computer networks that use the same protocol. Through a bridge, multiple LANs can be connected to form a larger and extended LAN.

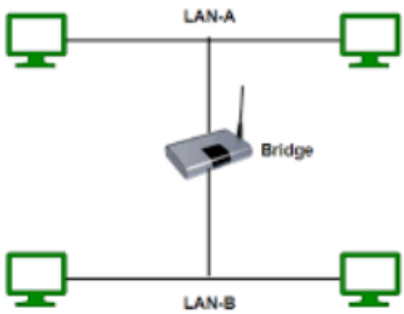


Figure 1.26Bridge

1.6.3.1Transparent Bridge

A transparent bridge in computer networking is a device that connects different network segments, allowing devices on those segments to communicate as if they were on the same network, without the devices themselves needing to be aware of the bridge's presence or the segmented nature of the network. It operates at the data link layer (Layer 2) of the OSI model and is primarily used in Ethernet environments.

1.6.3.2Source routing Bridge

A source routing bridge is a network device used to connect different network segments, where the sending device determines the specific path (or route) that data packets will take to reach their destination. Unlike transparent bridges, which learn routes automatically, source routing bridges require the

CamScanner

source device to embed routing information within the data packet itself. This approach is particularly useful in Token Ring networks and allows for more control.

1.6.4Switches

A switch, in the context of electrical engineering and networking, is a device that controls the flow of electricity or data. In electrical circuits, a switch acts as a gate, either allowing or blocking the flow of current. In networking, a switch connects multiple devices and enables them to communicate with each other within the same network.

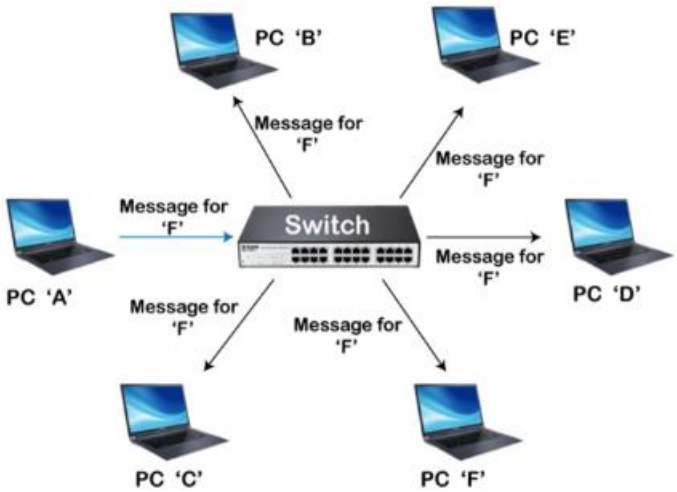


Figure 1.27switch

1.6.4.1Unmanaged switch

An unmanaged switch is a type of network switch that requires minimal or no configuration and is typically used for simple, small networks. It operates on a plug-and-play basis, automatically handling tasks like determining data rates and duplex settings. Unmanaged switches lack advanced features like VLAN support, traffic management, and security options, making them suitable for basic connectivity needs.

CamScanner

1.6.4.2Managed switch

A managed switch is a network device that provides advanced features and control over network traffic, unlike unmanaged switches which are plug-and-play with limited configuration options. Managed switches allow network administrators to monitor, configure, and manage individual ports and the overall network, enabling features like VLANs, Quality of Service (QOS), and remote management.

1.6.4.3Smart switch

Smart switches are light switches that can be controlled remotely through a smartphone app or voice commands, offering features like on/off control, dimming, and scheduling. They connect to your home's Wi-Fi network and often integrate with smart home systems.

1.6.4.4L2 switch

A Layer 2 switch is a networking device that operates at the Data Link layer (Layer 2) of the OSI model. It forwards data frames within a local area network (LAN) based on MAC addresses, which are unique identifiers for network interfaces. Unlike hubs, which broadcast data to all connected devices, Layer 2 switches intelligently direct traffic to the intended recipient, minimizing collisions and improving network performance.

1.6.4.5L3 switch

A Layer 3 switch, also known as a multilayer switch, combines the functionality of a traditional Layer 2 switch and a router. It can handle both Layer 2 switching (based on MAC addresses) and Layer 3 routing (based on IP addresses). This allows it to connect devices within the same subnet (like a regular switch) and also route traffic between different subnets or VLANs (like a router).

CamScanner

1.6.4.6PoE switch

A POE switch is a network switch that provides both data connectivity and electrical power to devices over standard Ethernet cables. This eliminates the need for separate power supplies and outlets for devices like IP cameras, wireless access points, and VoIP phones, simplifying installation and reducing costs.

1.6.4.7Gigbit switch

A Gigabit switch is a type of network switch, typically Ethernet-based, that allows devices to connect to a local area network (LAN) at speeds of up to 1 Gigabit per second (Gbps), or 1000 Megabits per second. It's an upgrade from older, slower Fast Ethernet switches (10/100 Mbps) and is commonly used in homes and businesses to connect various devices like computers, printers, and security cameras to the network.

1.6.4.8Rack-mounted switch

A rack-mounted switch is a type of network switch designed to be installed in a standard 19-inch rack, a framework used to organize and house multiple pieces of networking equipment like servers, routers, and other switches. These switches are typically used in data centers, server rooms, or other environments where multiple devices need to be connected and managed efficiently.

1.6.4.9Desktop switch

Desktop switches are small and lightweight and can be placed on a table, shelf, or other flat surface. Their small size makes them ideal for home offices, small businesses, or temporary setups. Rack-mount switches: Rack-mount switches are larger, more rugged, and fit into a standard 19-inch server rack.

CamScanner

1.6.4.10Modular switch

Modular switch is a type of network switch designed to be installed in a standard 19-inch rack, and it features a modular design allowing for the addition of various line cards or modules to customize its capabilities. This design enables flexibility in terms of port density, speed, and functionality, making it suitable for large and growing networks.

1.6.5Routers

A router is a networking device that forwards data packets between computer networks. It connects multiple networks, like your home network to the internet, and directs data traffic to its intended destination. Essentially, it's the traffic controller of the internet, ensuring information gets where it needs to go.

The router connects all devices on your home network and allows them to communicate. It also allows those devices to connect to the internet. Other advantages of a router include Firewall security .A router can provide some protection against outside threats by acting as a firewall.

A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

CamScanner

1.6.6Modem

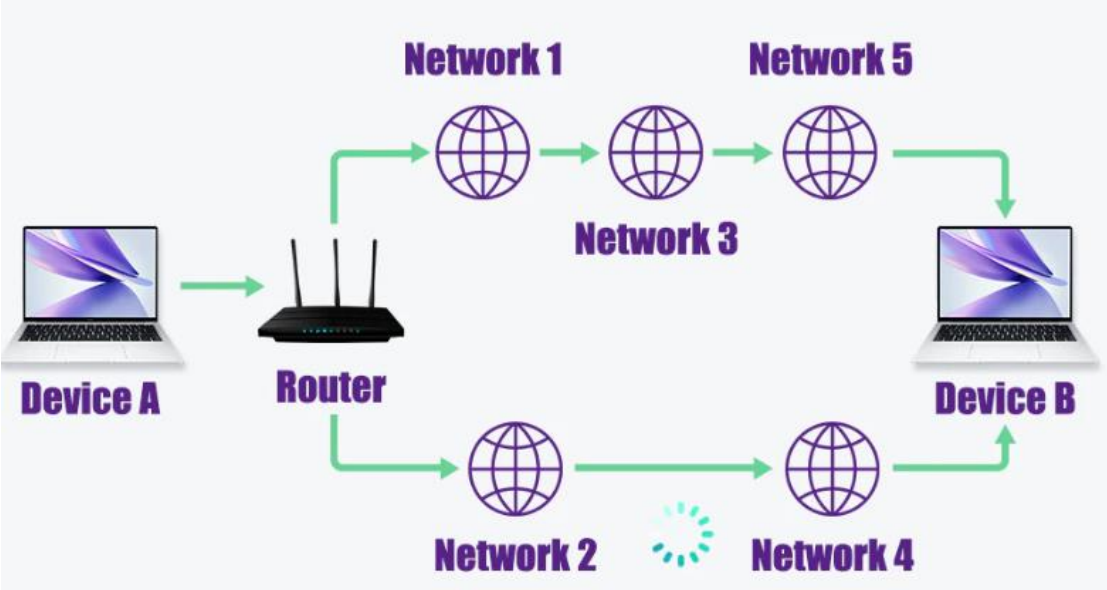


Figure 1.28Router

A modem is a device that connects your home network to the internet by translating digital signals from your devices into a format that can be transmitted over internet cables or other media, and vice versa. Essentially, it acts as a bridge between your home network and your internet service provider (ISP).

1.6.7Network interface card (NIC)

NIC can refer to a few things. In computer networking, it stands for Network Interface Card, a hardware component that allows a computer to connect to a network. It's also an abbreviation for National Informatics Centre, the technology partner of the Government of India. Additionally, (NIC) can be slang for nicotine.

In a computing device, a NIC contains the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi.

CamScanner

1.6.8Server

A server is a computer or system that provides resources, data, services, or programs to other computers (clients) over a network. Servers can be hardware or software, and they play a crucial role in various applications, including web hosting, email services, and data storage.

Technically, a server is a computer that runs a program that allows you to connect to other computers over the Internet. So it's kind of like a web browser, but it's more powerful. But really, the word server is just a term used to describe a computer that runs something. [5]

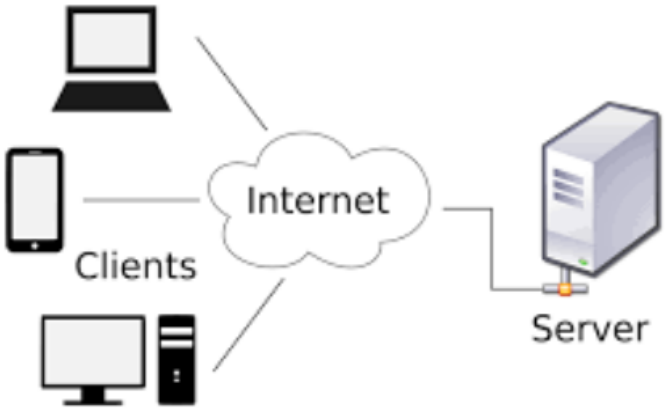


Figure 1.29Server

CamScanner

Chapter2: Switching

2.1 Introduction

A switch, in the context of computer networking, is a device that connects multiple devices within a local area network (LAN) allowing them to communicate with each other. It intelligently forwards data packets only to the intended recipient, maximizing network efficiency and security. In electrical engineering, a switch is a component that can break or complete an electrical circuit, controlling the flow of current.

2.2 Process of switching

- **Learn MAC address:** switch can read the header of the frame (source mac and destination mac).
- **Take decision:** switch find the best path with less cost according to root switch.
- **Switching table update:** switch store the source mac first and finally the destination mac in the mac table to forward the data without broadcast process always.
- **Loop prevention:** in the multiple paths to the root this cause loop so switch prevent it by making this paths BLK expect one path with less cost according to root switch.

CamScanner

2.3 Switch port

2.3.1Types of switch port

Switch port are classified into the following types

- **Access port:** An access port on a network switch is a port that connects to a single end device (like a computer or printer) and is configured to carry traffic for only one specific VLAN. It's designed for simple connections where devices don't need to handle VLAN tagging.

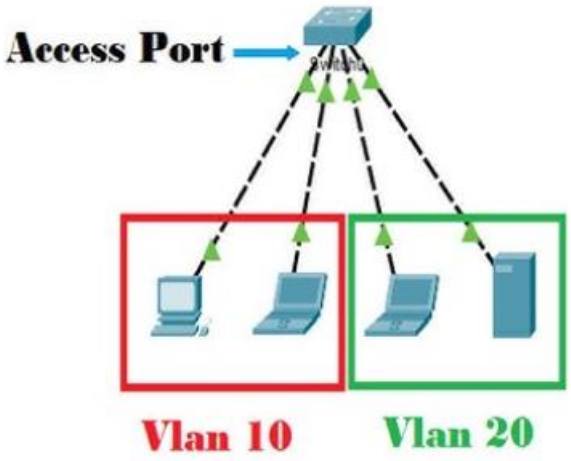


Figure 2.1 Access ports

Trunk port: A trunk port is a network switch port configured to carry traffic from multiple VLANs (Virtual Local Area Networks) simultaneously. Unlike access ports, which handle traffic for a single VLAN, trunk ports use VLAN tagging to differentiate and direct traffic to the correct VLAN as it traverses the network. This allows for the extension of VLANs across multiple switches, enabling communication between devices in different VLANs on

CamScanner

different switches. The primary difference between trunk ports and access ports is their method of managing VLAN traffic. While trunk ports support multiple VLANs using tagging methods such as IEEE 802.1Q, access ports are dedicated to a single VLAN and do not use tags.

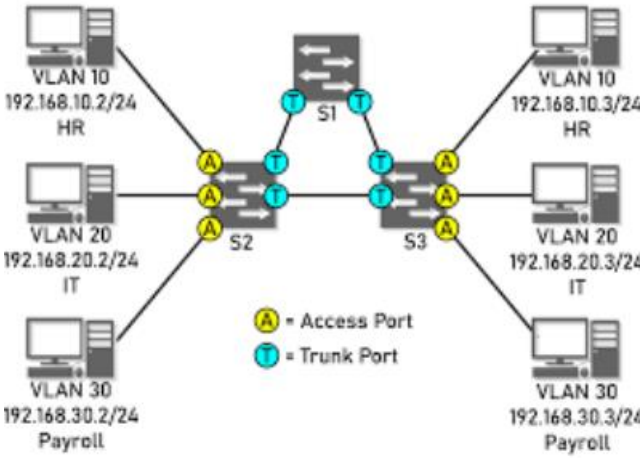


Figure 2.2 Trunk ports& Access port

2.3.2Number of switch port

Switches can have 5-port to 52-port configurations. Fixed-configuration switches typically come with five, eight, ten, sixteen, twenty-four, eighteen, forty-eight, or fifty-two ports. You should think about the number of users your network can accommodate when determining how many ports you will need. [6]

2.4 Layer 2 and Layer 3 switches

2.4.1 Layer 2 switches

CamScanner

A layer 2 switch, also known as an Ethernet switch, functions at the data link layer (Layer 2) of the OSI model. Its primary role is to forward data packets (frames) between devices within the same local area network (LAN) based on MAC addresses. It learns these addresses and builds a table to efficiently direct traffic, reducing collisions and improving network performance. Layer 2 switches enable the use of dedicated LAN segments for each attached end system, minimizing collisions and delay. They perform all the operations of typical bridges but employ specialized hardware for frame forwarding, often using cut-through routing techniques.

2.4.2 Layer 3 switches

A Layer 3 switch combines the functions of a switch and a router, enabling it to handle both Layer 2 (switching) and Layer 3 (routing) operations.

It can switch data packets at high speed within a local network (VLAN or subnet) like a traditional switch, while also routing packets between different subnets or VLANs, similar to a router. This makes it ideal for larger networks with multiple VLANs where efficient inter-VLAN routing is needed. A Layer 3 switch combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speed.

It can support routing protocols, inspect incoming packets, and may even make routing decisions supporting source and destination addresses. Layer 3 switches can handle multiple tasks, including switching, routing, and Layer 2 functions, such as bridging at each interface.

CamScanner

Also, they can manage data flow and limit broadcast traffic. Being extremely robust and scalable, Layer 3 is perfect for high-traffic networks.

2.5Subnetting

Subnetting is essential for efficient network management, enhancing performance, security, and organization. By dividing a larger network into smaller, manageable subnets, it reduces network congestion, optimizes IP address allocation, and simplifies routing. This segmentation also improves security by isolating network segments and controlling traffic flow.

Subnetting limits the IP address usage to within a few devices. This allows an engineer to use subnetting to create sub-networks, sorting data so that it can travel without touching every part of the more complex routers. To do this, an engineer needs to match each IP address class to a subnet mask.

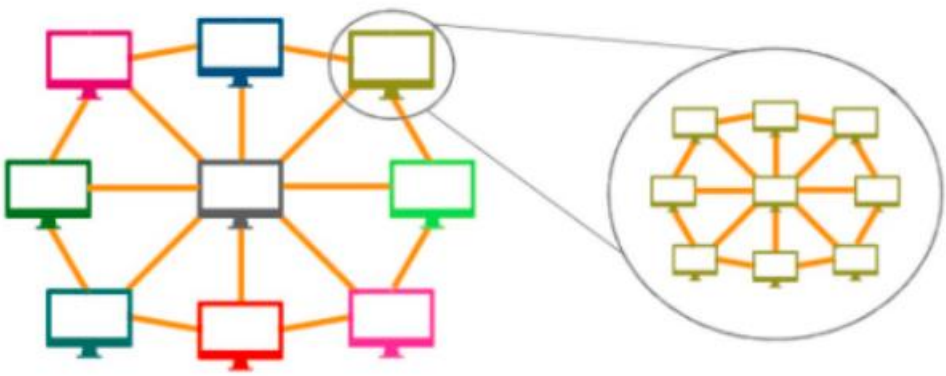


Figure 2.3Subnetting

CamScanner

2.5.1IP address

An IP address is a unique numerical label assigned to devices connected to a computer network that uses the Internet Protocol for communication. It's essentially the online address of your device, like a street address for your computer, allowing it to send and receive data over the internet.

IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network. In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication.

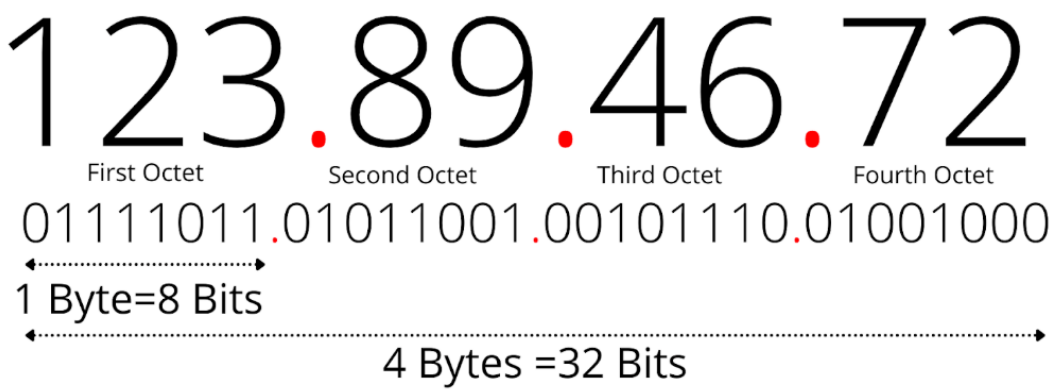


Figure 2.4IP format

2.5.1.1 IP V4 &IPV6 address

- **IPV4:** An IPv4 address is a 32-bit numerical label assigned to devices participating in a computer network that uses the Internet Protocol version 4. It's commonly represented in dotted-decimal

CamScanner

notation, like 192.168.1.1, where each number is an 8-bit octet ranging from 0 to 255.

- **IPV6:** An IPv6 address is a 128-bit address used to identify and locate network interfaces in IPv6 networks. It is written as eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IPv 6 addresses are designed to replace the older IPv4 addresses, which are running out due to the increasing number of internet-connected devices.

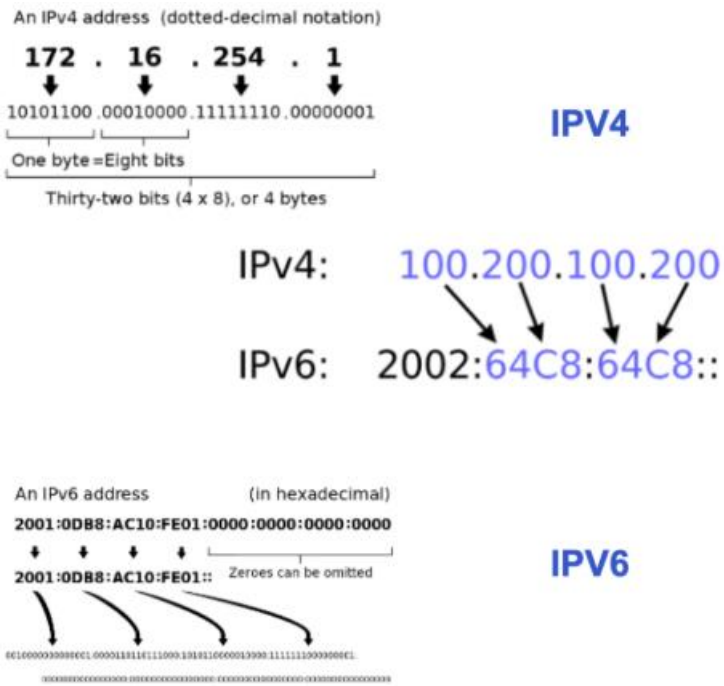


Figure 2.5IPV6&IPV4

2.5.1.2 Types of IP address

- **Public IP:** A public IP address is a unique address that identifies your device on the internet, allowing you to connect to websites and other online services. Your Internet Service Provider

CamScanner

(ISP) assigns this address to your router, which then shares it with the devices on your network.

- **Private IP:** A private IP address is a unique numerical label assigned to devices within a local network, such as your home or office network. These addresses are not directly accessible from the internet and are used for communication within the local network only.
- **Static IP:** A static IP address is a manually configured signifier assigned to a device that remains consistent and cannot change across multiple network sessions. All devices that use IP addresses, such as desktop computers, laptops, routers, and tablets, can be configured to have static IP addresses.
- **Dynamic IP:** A dynamic IP address is an IP address that changes periodically, rather than remaining constant. Internet service providers (ISPs) typically assign dynamic IP addresses to home users and some businesses using DHCP (Dynamic Host Configuration Protocol). This means the IP address assigned to a device can change each time it connects to the network or after a certain lease time expires.

CamScanner

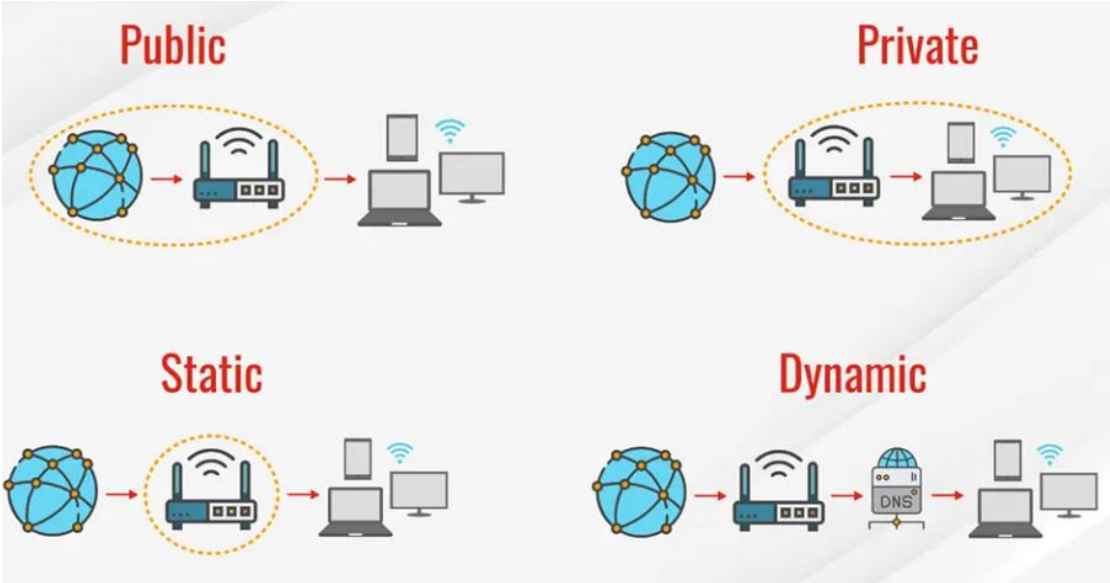


Figure 2.6 Types of IP

2.5.1.3 Classful IP

Classful addressing is an IPv4 addressing architecture that divides addresses into five groups. Prior to classful addressing, the first eight bits of an IP address defined the network a given host was a part of. This would have had the effect of limiting the internet to just 254 networks.

1- Class A:1-126 (the last lift octet) with mask 255.0.0.0
   0 is reserved to **gateway of last resort**, 127 is reserved for **TCP/IP.**
2- Class B:128-191(the last lift octet) with mask 255.255.0.0
3- Class C 192-223(the last lift octet) with mask 255.255.255.0
4- Class D 224-239(the last lift octet) for multicast.
5- Class E 240-254 (the last lift octet) for future use
   255 is reserved to **direct broadcast.**

CamScanner

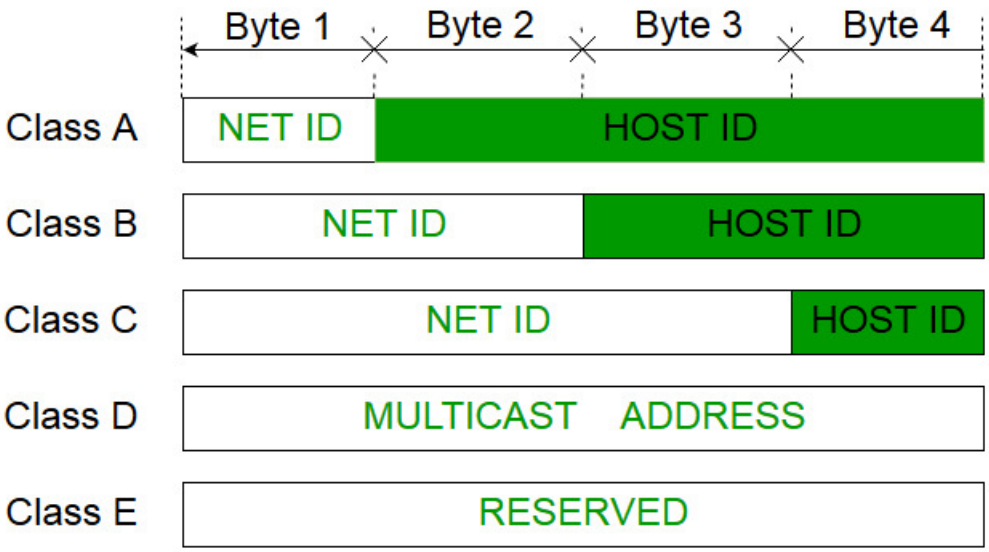


Figure 2.7 IP classes

2.5.1.4 Common IP address threats

Common IP address threats include DDoS attacks, IP spoofing, phishing, malware infections, and online stalking. Hackers can exploit IP addresses to disrupt services, steal data, or impersonate users.

2.5.1.5 Solutions for consumption IP address

There are solutions that aim to consumption IPV4:

1- **IPV6:**IPV4 contain 32bit while IPV6 contain 128 bit this increase the number of IPs.
2- **NAT** (Network address translation): Network Address Translation (NAT) is a networking technique that allows multiple devices on a private network to share a single public IP address when communicating with devices on a public network like the internet. It essentially acts as a translator,

CamScanner

converting internal (private) IP addresses to a single public IP address for outgoing traffic and translating the public IP address back to the appropriate internal IP for incoming traffic.

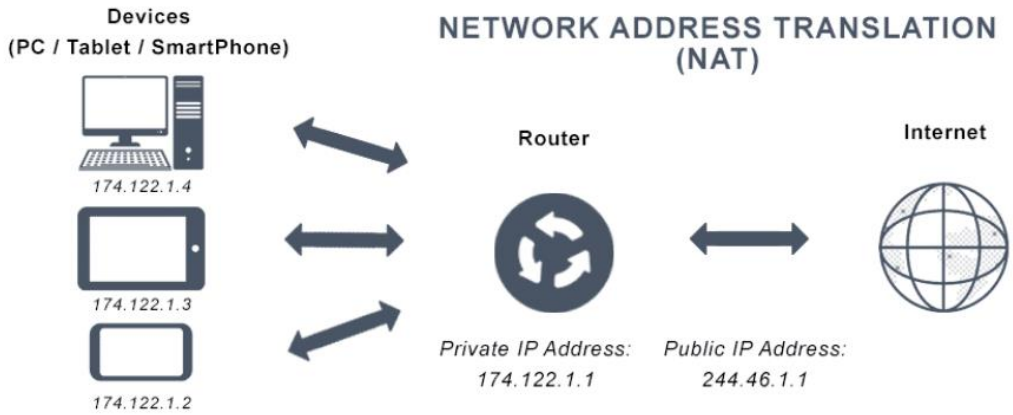


Figure 2.8 NAT(Network address Translation)

3-**FLSM** (Fixed-Length Subnet Mask): is a subnetting technique where all subnets within a network have the same subnet mask and therefore the same number of usable IP addresses. This means each subnet has the same size.

4-VLSM (variable length subnet mask):Is a technique used in computer networking to divide an IP address space into subnets of varying sizes.

2.5.2Subnet mask

CamScanner

A subnet mask is a 32-bit number that divides an IP address into network and host portions, enabling devices to determine whether another device is on the same local network or a remote network. It essentially separates the network address from the host address within an IP address. To calculate a subnet mask, network administrators determine the number of bits needed for both the network and host portions of an IP address. Once network admins determine the number of network bits, they set those bits to ones and the remaining bits to zeros for the host portion.

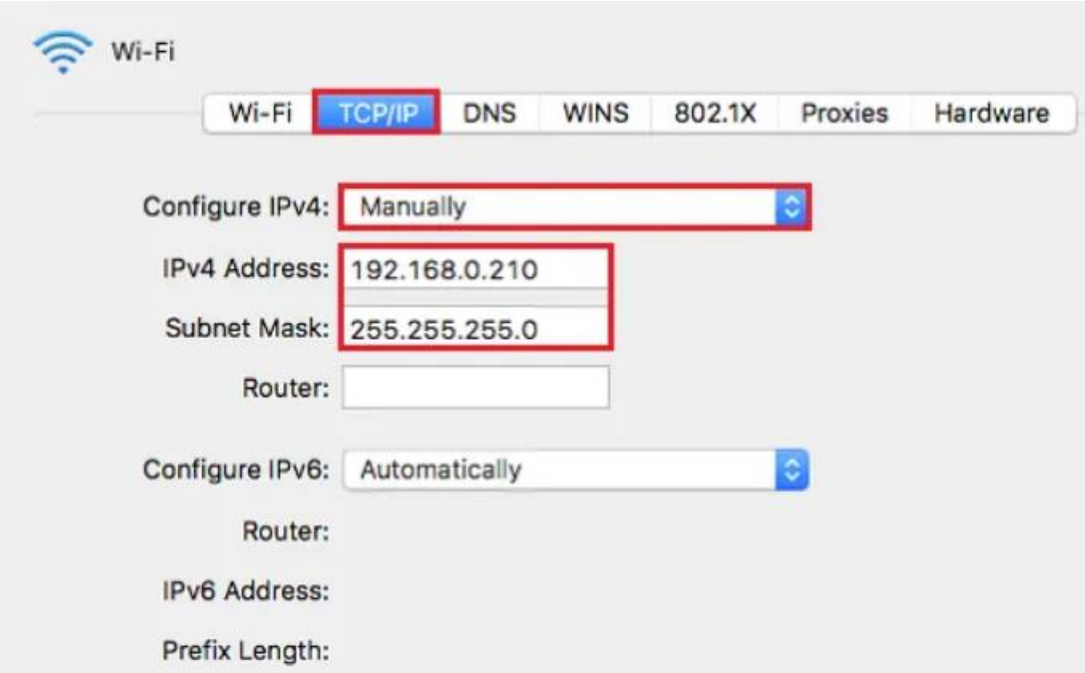


Figure 2.9 Subnet mask

2.5.2.1 Point to point Subnet mask

A point-to-point subnet is a network configuration designed for exactly two connected devices, often used in links between routers. It uses a subnet mask (like /30) that allows for only two usable IP addresses, eliminating the need for separate network and broadcast addresses. This approach optimizes address space utilization on these dedicated links. [7]

CamScanner

Figure 2.10 point to point connect

2.6VLANs (virtual LANs)

A VLAN, or Virtual LAN, is a logical way to divide a physical network into multiple broadcast domains. It allows network administrators to group devices together based on function, security requirements, or other criteria, regardless of their physical location. This segmentation enhances network management, improves security, and optimizes traffic. VLANs create separate broadcast domains within a single physical network.

This means that devices within the same VLAN can communicate with each other as if they were on a separate network, while devices in different VLANs cannot communicate directly unless routed. VLANs are not tied to physical locations. Devices can be added to or removed from a VLAN without needing to physically move them. VLANs are typically implemented using switches that support VLAN tagging. Each network frame is tagged with a VLAN ID, which the switch uses to determine which VLAN the frame belongs to.

CamScanner

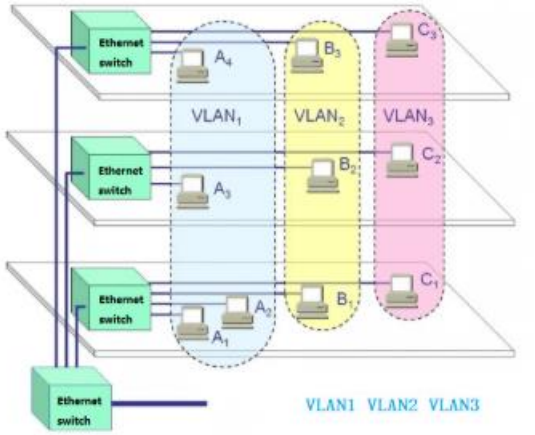


Figure 2.11 VLAN

2.6.1VLANs ranges:

- **VLAN 0, 4095:** These are reserved VLAN which cannot be seen or used.
- **VLAN 1**: it's the default VLAN of switch. All ports by default assign in VLAN 1. This VLAN cannot by deleted or edited but can be used.
- **VLAN 2-1001**: This is the normal VLAN range .we can create, edit and delete these VLANs.
- **VLAN 1002-1005**: These area CISCO defaults for FDDI and token rings. These VLANs cannot be deleted.
- **VLAN 1006-4094**: This is the extended range of VLAN.

2.6.2VLANs features:

- **Easier Configuration:** VLANs simplify network management by allowing administrators to group devices logically for configuration and troubleshooting purposes.
- **Flexibility:** VLANs can be easily reconfigured as network needs change.

CamScanner

- **Accommodates Growth:** VLANs can be easily scaled to accommodate network growth by adding or modifying VLANs as needed.
- **Reduced Hardware Needs:** VLANs can reduce the need for additional physical hardware by allowing multiple logical networks to share the same physical infrastructure.

2.6.3VLANs Application:

- **Cloud Computing:**

VLANs are crucial for isolating different tenants and their resources in cloud environments.

- **Voice over IP (VoIP):**

VLANs separate voice traffic from data traffic, improving call quality and reducing network congestion.

- **Gaming:**

VLANs can prioritize gaming traffic, ensuring a smoother online gaming experience.

- **Internet of Things (IOT):**

VLANs can isolate IOT devices from the main network, enhancing security and reducing potential disruptions.

- **Remote Access:**

VLANs provide secure remote access to cloud-based applications and resources.

- **Large Enterprises:**

VLANs help organize and manage traffic for different departments, improving efficiency and security.

2.6.4 VLANs Types:

1- Data VLAN:

Also known as a user VLAN, it is the most common type and is used to separate and organize network traffic based on user

CamScanner

groups, departments, or security requirements. It isolates user data traffic from other types of traffic like voice or management traffic.

2-Voice VLAN:

Specifically has been designed to handle voice traffic, particularly for VoIP (Voice over IP) phones .Prioritizes voice traffic over other network traffic to ensure quality and reliability.

3- Management VLAN:

Dedicated to network management and administration tasks, such as SNMP, SSH, and Telnet .Recommended for sensitive management activities.

4-Default VLAN:

Typically, VLAN 1 on most switches, where all ports are members by default until explicitly assigned to another VLAN.

5- Native VLAN:

A VLAN assigned to untagged traffic on a trunk port. In 802.1 Q trunking , the native VLAN carries untagged frames.

6- Port-based VLANs:

VLAN membership is determined by the physical port on the switch .Each port is assigned to a specific VLAN.

7- Private VLANs:

A more advanced type that divides a primary VLAN into isolated or community VLANs to enhance security and control traffic flow.[8]

2.7 STP (spanning tree protocol)

CamScanner

` The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology in switched networks. It accomplishes this by dynamically disabling redundant links, preventing broadcast storms and network instability that can occur when multiple paths exist between network devices.

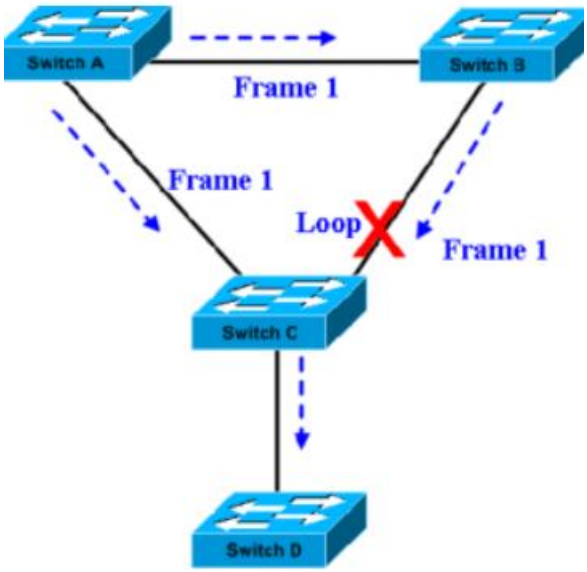


Figure 2.12 STP

2.7.1 STP features

1-Loop Prevention:

In a network with redundant links, a broadcast storm can occur when a data packet is repeatedly forwarded between switches, causing network congestion and potential failure. STP prevents this by using an algorithm to identify loops and selectively blocking certain ports to create a tree-like topology.

2-Redundancy:

CamScanner

While preventing loops, STP also allows for the inclusion of redundant links, which can be activated if a primary link fails, ensuring network availability.

3-Key Concepts:

- **Root Bridge:** The central switch in the spanning tree, determined by a comparison of bridge IDs.
- **Root Port:** The port on a non-root switch that offers the shortest path to the root bridge.
- **Designated Port:** The port on a segment that offers the shortest path to the root bridge.
- **Blocked Port:** Redundant ports that are disabled to prevent loops.

4-Port States:

Ports in STP transition through different states (blocking, listening, learning, forwarding, disable) as the protocol establishes the loop-free topology.

5-Evolution:

STP (IEEE 802.1D) has evolved into Rapid Spanning Tree Protocol (RSTP - IEEE 802.1w) and Multiple Spanning Tree Protocol (MSTP), offering faster convergence times and improved features.

2.7.2 STP states:

- **Blocking:**

  The Initial state for all ports is enabled. Ports in this state do not forward frames and do not learn MAC addresses, but they do listen for BPDUs (Bridge Protocol Data Units).

- **Listening:**

CamScanner

Ports in the listening state still don't forward frames, but they begin to process BPDUs to determine their role in the network topology (root port, designated port, or blocked port).

- **Learning:**

  Ports in this state are preparing to forward traffic. They still don't forward frames, but they start learning MAC addresses and populate the MAC address table.

- **Forwarding:**

  This is the normal operational state where ports forward frames and continue to learn MAC addresses.

- **Disabled:**
  This state occurs when a port is administratively disabled or encounters an error. In this state, the port does not forward frames, learn MAC addresses, or process BPDUs.

-STP introduced a few terms which are frequently used

- **BPDU (Bridge protocol data unit):** A BPDU (Bridge Protocol Data Unit) is a specialized message used in network protocols like Spanning Tree Protocol (STP) and its variants (RSTP, MSTP) to manage and maintain the network topology of switched networks. These messages are exchanged between switches to discover each other, determine their roles, and prevent network loops.
- **Root Port:** a root port is the single, best path from a non-root bridge (switch) to the root bridge. It's the port on a non-root switch that offers the lowest cost path to reach the root bridge. Each non-root bridge has only one root port.
- **Designated Port:** A root port is the single, best path from a non-root bridge (switch) to the root bridge. It's the port on a non-root switch that offers the lowest cost path to reach the root bridge. Each non-root bridge has only one root port.

CamScanner

- **Alternated Port:** Acts as a backup path to the root bridge, taking over if the primary root port is blocked. It's essentially a redundant connection that ensures network connectivity is maintained even if the designated path to the root bridge is interrupted.
- **Discarding port state:** In Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP), the discarding state indicates that a port is not forwarding user traffic or learning MAC addresses. This state is used to prevent loops in the network topology and can be a transitional state or a permanent state for certain port roles.
- **Forwarding port:** A state where a switch port is actively forwarding data packets. This means the port is both receiving and transmitting data, playing an active role in forwarding traffic across the network. It's the final, stable state a port reaches after transitioning through other states like listening and learning.

2.7.3STP Algorithm:

- **Root Bridge Election:**

  STP elects a root bridge (or root switch) based on the bridge ID (BID), which includes a priority value and the switch's MAC address.

- **Root Port Selection:**

  Each non-root switch then determines its root port, which is the port closest to the root bridge (lowest path cost).

- **Designated Port Selection:**
  Finally, designated ports are selected on each network segment (link) based on the lowest path cost to the root bridge. Other ports on that segment are placed in a blocking state.

CamScanner

2.7.4Types of spanning tree protocol:

- **Standard STP (IEEE 802.1D):**

  This is the original STP standard. It's known for its simplicity but has slower convergence times.

- **Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w):**

  RSTP is an improvement over STP, offering faster convergence times and better performance.

- **Per-VLAN Spanning Tree (PVST):**

  This Cisco proprietary protocol creates a separate spanning tree instance for each VLAN, allowing for more flexible and efficient traffic forwarding.

- **Rapid Per-VLAN Spanning Tree (RPVST):**

  An enhancement of PVST, it combines the benefits of PVST with the faster convergence of RSTP.

- **Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s):**
  MSTP maps multiple VLANs to a single spanning tree instance, offering a balance between performance and complexity. It allows for more efficient use of network resources compared to PVST.[9]

2.8RSTP (Rapid spanning tree Protocol)

Rapid Spanning Tree Protocol (RSTP), defined in IEEE 802.1w, is a network protocol that prevents loops in Ethernet networks by creating a loop-free logical topology. It is an enhanced version of the original Spanning Tree Protocol (STP) and provides faster convergence, meaning it can react to network changes or failures more quickly.

CamScanner

2.8.1RSTP features:

- **Loop Prevention:**

  Like STP, RSTP prevents loops in switched networks by blocking redundant paths.

- **Faster Convergence:**

  RSTP achieves faster convergence (the time it takes to establish a stable, loop-free topology) than STP by introducing new port roles and convergence behaviors.

- **Backwards Compatibility:**

  RSTP is designed to be backwards compatible with STP, meaning it can coexist with older STP devices in the same network.

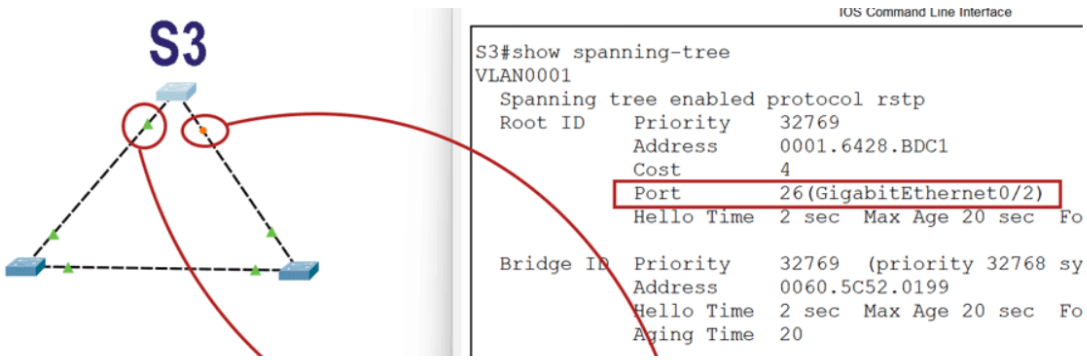
- **Port Roles:**

  RSTP introduces new port roles beyond the root and designated ports found in STP. These include alternate and backup ports, which act as backups to the root and designated ports, respectively.

- **Edge Ports:**

  RSTP also introduces the concept of edge ports, which are directly connected to end stations and can immediately transition to the forwarding state, skipping the listening and learning stages.

- **IEEE Standard:**
  RSTP is defined by the IEEE standard 802.1w.



CamScanner

2.9MSTP (Multiple spanning tree Protocol)

The Multiple Spanning Tree Protocol (MSTP), defined by IEEE 802.1s, is a network protocol that enhances network redundancy and load balancing by allowing multiple spanning trees to operate on the same physical network. It groups VLANs into spanning tree instances and regions, enabling different VLANs to utilize diverse forwarding paths, improving fault tolerance and resource utilization.

2.9.1MSTP features:

- **Multiple Spanning Trees:**

  MSTP allows the creation of multiple independent spanning trees, unlike the original Spanning Tree Protocol (STP) which uses a single spanning tree for the entire network.

- **MST Regions:**

  MSTP organizes switches into regions, where all switches within a region share the same MST configuration (name, revision number, and VLAN-to-instance mapping).

- **VLAN Mapping:**

  MSTP maps VLANs to specific spanning tree instances, allowing different VLANs to follow different paths within the network, enabling load balancing and redundancy.

- **Compatibility:**

  MSTP is compatible with both STP and Rapid Spanning Tree Protocol (RSTP), ensuring interoperability with older devices.

- **Fault Tolerance:**

CamScanner

By using multiple spanning trees, MSTP provides improved fault tolerance. If one instance (forwarding path) fails, other instances can continue to operate, minimizing network downtime.

- **Load Balancing:**
  MSTP allows for load balancing by distributing traffic across different spanning tree instances, optimizing network performance and resource utilization. [10]

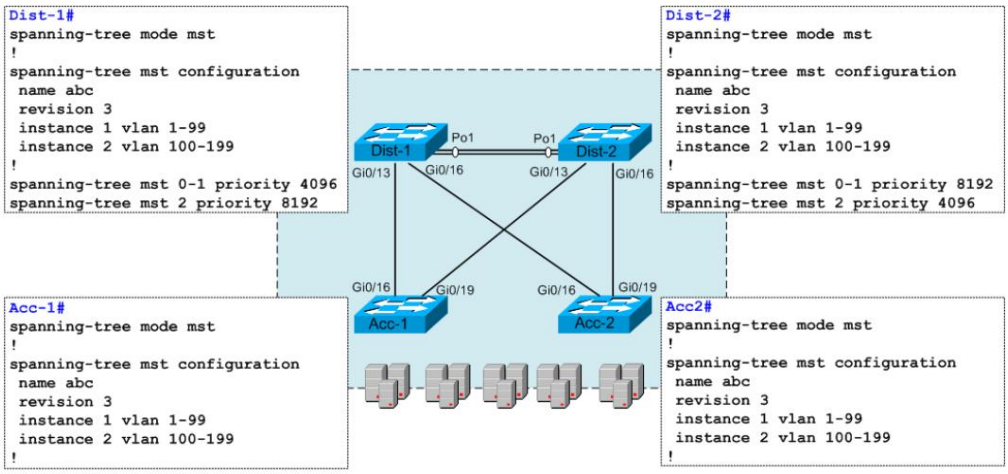


Figure 2.14 MST

2.10Etherchannel

It is a link aggregation, is a technology that groups multiple physical Ethernet links into a single logical link, increasing bandwidth and providing redundancy. This logical link, referred to as a port channel or ether channel bundle, acts as a single, higher-bandwidth connection between network devices.

CamScanner

2.10.1Etherchannel feature

- **Increased Bandwidth:** By combining multiple links, Ether Channel provides a higher aggregate bandwidth than a single link.
- **Redundancy:** If one physical link in the Ether Channel fails, the remaining links continue to operate, providing a fault-tolerant connection.
- **Load Balancing:** Traffic is distributed across the active links within the Ether Channel, improving overall network performance.

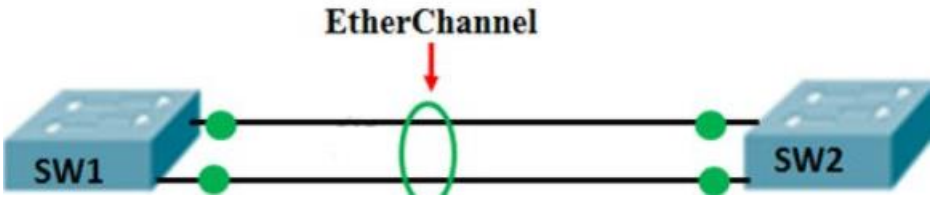


Figure 2.15 Ether channel

2.10.2Etherchannel Mechanism

To create ether channel in the network all of the interfaces in the group should have

- Same Duplex
- Same switch port mode
- Same speed
- Same VLAN configuration

  Ether channel has more one mechanism to determine the forwarding of data over all paths in the group
- Source MAC
- Destination MAC
- Source and destination MAC

CamScanner

- Source IP address
- Destination IP address
- Source and destination IP address
- Source TCP/IP port
- Destination TCP/IP port
- Source and destination TCP/IP port

2.10.3Etherchannel Work

- **PAGP(Port aggregation protocol):**

  Port Aggregation Protocol (PAGP) is a Cisco-proprietary protocol used for automatically creating Ether Channels, which aggregate multiple physical Ethernet links into a single logical link, increasing bandwidth and redundancy. It functions by exchanging PAGP packets between switch ports to negotiate and establish the Ether Channel.

- **LACP(link aggregation control protocol):**

  LACP, or Link Aggregation Control Protocol, is a standard defined by IEEE 802.3ad that allows network devices to dynamically negotiate and configure link aggregation groups (LAGs). LACP simplifies the process of combining multiple physical links into a single logical link, increasing bandwidth, reliability, and load balancing. [11]

CamScanner

Chapter3: Routing

3.1Path Determination

When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. This is known as routing. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network. Each network that a router connects to typically require a separate interface, but this may not always be the case.

The primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination.

3.1.1Buliding routing table

1-Directly Connected Networks: Added to the routing table when a local interface is configured with an IP address and subnet mask (prefix length) and is active (up and up).

2-Remote Networks: Networks that are not directly connected to the router. Routers learn about remote networks in two ways:

- **Static routes** - Added to the routing table when a route is manually configured.
- **Dynamic routing protocols** - Added to the routing table when routing protocols dynamically learn about the remote network.
- **Default Route:** Specifies a next-hop router to use when the routing table does not contain a specific

CamScanner

route that matches the destination IP address. The default route can be entered manually as a static route, or learned automatically from a dynamic routing protocol.

A default route has a /0 prefix length. This means that no bits need to match the destination IP address for this route entry to be used. If there are no routes with a match longer than 0 bits, the default route is used to forward the packet. The default route is sometimes referred to as a gateway of last resort.

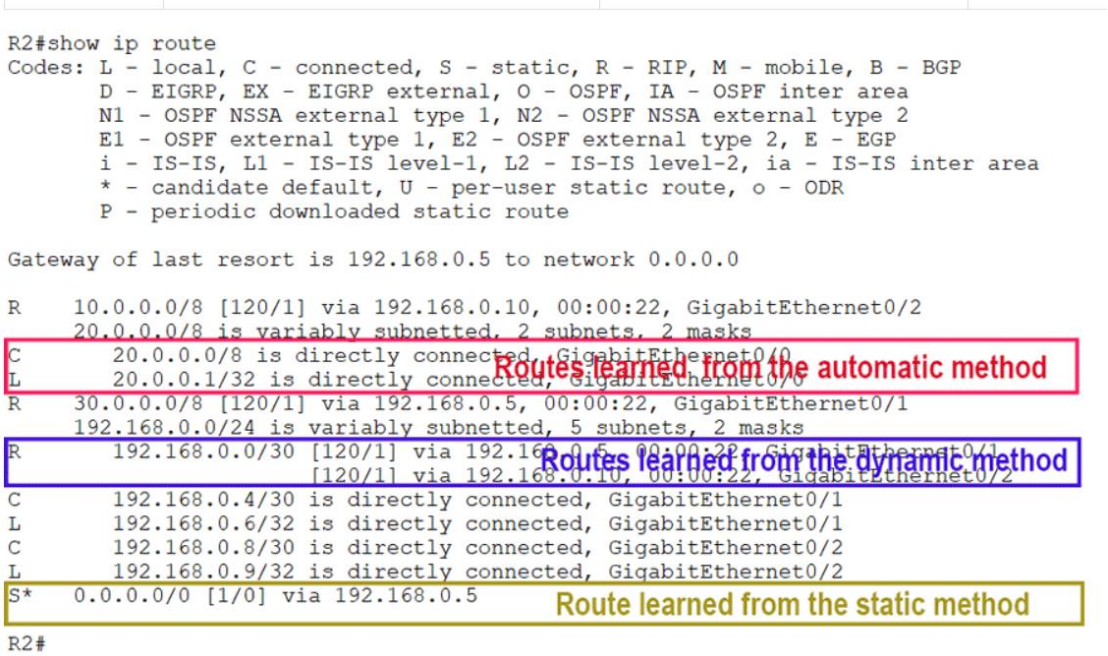

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 192.168.0.5 to network 0.0.0.0
R 10.0.0.0/8 [120/1] via 192.168.0.10, 00:00:22, GigabitEthernet0/2
20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 20.0.0.0/8 is directly connected, GigabitEthernet0/0
L 20.0.0.1/32 is directly connected, GigabitEthernet0/0
Routes learned from the automatic method
R 30.0.0.0/8 [120/1] via 192.168.0.5, 00:00:22, GigabitEthernet0/1
192.168.0.0/24 is variably subnetted, 5 subnets, 2 masks
R 192.168.0.0/30 [120/1] via 192.168.0.5, 00:00:22, GigabitEthernet0/1
[120/1] via 192.168.0.10, 00:00:22, GigabitEthernet0/2
Routes learned from the dynamic method
C 192.168.0.4/30 is directly connected, GigabitEthernet0/1
L 192.168.0.6/32 is directly connected, GigabitEthernet0/1
C 192.168.0.8/30 is directly connected, GigabitEthernet0/2
L 192.168.0.9/32 is directly connected, GigabitEthernet0/2
S* 0.0.0.0/0 [1/0] via 192.168.0.5
Route learned from the static method
R2#

Figure 3.1Routing table

3.2Pcaket Forwarding

- The data link frame with an encapsulated IP packet arrives on the ingress interface.
- The router examines the destination IP address in the packet header and consults its IP routing table.

CamScanner

- The router finds the longest matching prefix in the routing table.
- The router encapsulates the packet in a data link frame and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.

  However, if there is no matching route entry the packet is dropped.

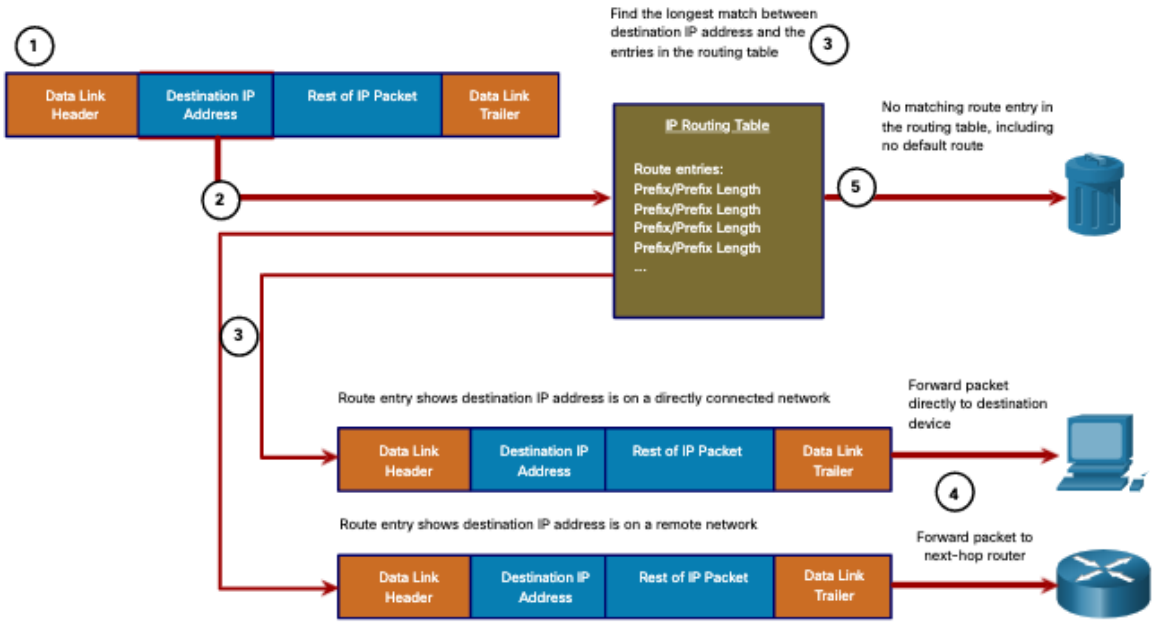


Figure 3.2Encapsulation&Dencapsulation

After a router has determined the best path, it could do the following:

Forward the Packet to a Device on a Directly Connected Network

- If the route entry indicates that the egress interface is a directly connected network, the packet can be forwarded directly to the destination device. Typically this is an Ethernet LAN.

CamScanner

- To encapsulate the packet in the Ethernet frame, the router needs to determine the destination MAC address associated with the destination IP address of the packet. The process varies based on whether the packet is an IPv4 or IPv6 packet.

Forward the Packet to a Next-Hop Router

- If the route entry indicates that the destination IP address is on a remote network, meaning a device on network that is not directly connected. The packet must be forwarded to the next-hop router. The next-hop address is indicated in the route entry.
- If the forwarding router and the next-hop router are on an Ethernet network, a similar process (ARP and ICMPv6 Neighbor Discovery) will occur for determining the destination MAC address of the packet as described previously. The difference is that the router will search for the IP address of the next-hop router in its ARP table or neighbor cache, instead of the destination IP address of the packet.

Drop the Packet - No Match in Routing Table

- If there is no match between the destination IP address and a prefix in the routing table, and if there is no default route, the packet will be dropped.

CamScanner

3.3Basic Router Configuration Review

The topology in the figure will be used for configuration and verification examples. It will also be used in the next topic to discuss the IP routing table.

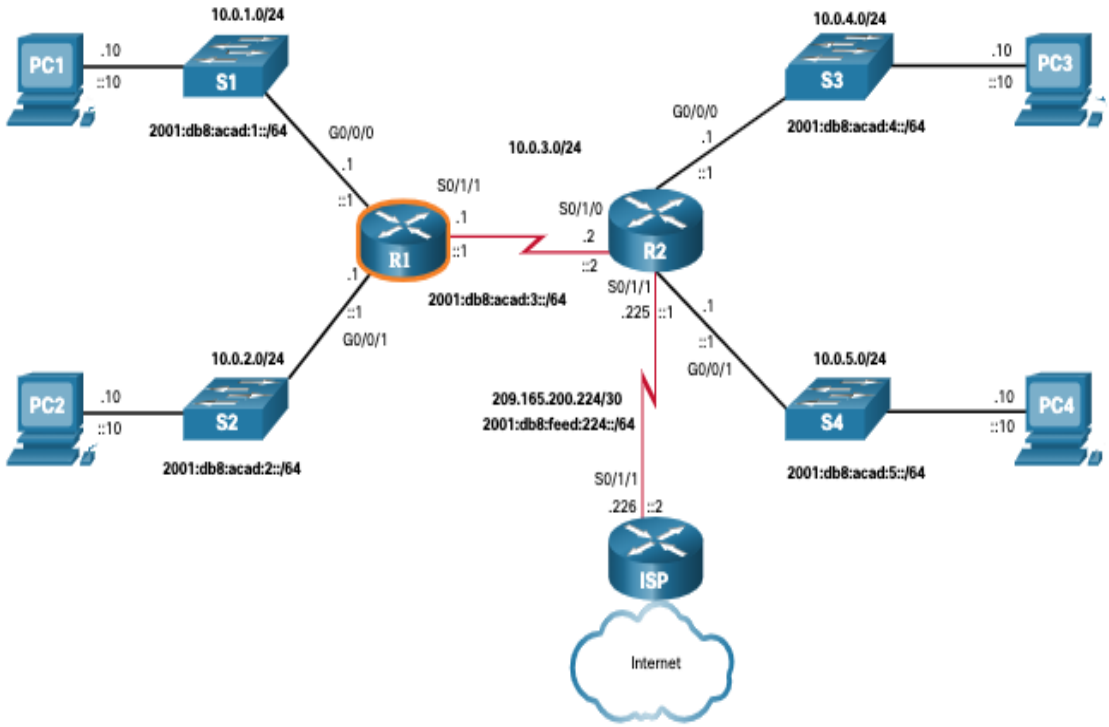


Figure 3.3 Routing Topology

The Configuration:

Router> **enable**

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router (config) # **hostname R1c**

R1 (config) # **enable secret class**

R1 (config) # **line console 0**

CamScanner

R1 (Config-line) # **logging synchronous**

R1 (config-line) # **password cisco**

R1 (config-line) # **login**

R1 (config-line) # **exit**

R1 (config) # **interface gigabitethernet 0/0/0**

R1 (config-if) # **description Link to LAN 1**

R1 (config-if) # **ip address 10.0.1.1 255.255.255.0**

R1 (config-if) # **no shutdown**

R1 (config-if) # **exit**

R1 (config) # **interface gigabitethernet 0/0/1**

R1 (config-if) # **description Link to LAN 2**

R1 (config-if) # **ip address 10.0.2.1 255.255.255.0**

R1 (config-if) # **no shutdown**

R1 (config-if) # **exit**

R1 (config) # **interface serial 0/1/1**

R1 (config-if) # **description Link to R2**

R1 (config-if) # **ip address 10.0.3.1 255.255.255.0**

R1 (config-if) # **no shutdown**

R1 (config-if) # **exit**

CamScanner

3.4Route Source

A routing table contains a list of routes to known networks (prefixes and prefix lengths). The source of this information is derived from the following:

- Directly connected networks
- Static routes
- Dynamic routing protocols

The source for each route in the routing table is identified by a code. Common codes include the following:

- **L** - Identifies the address assigned to a router interface.
- **C** - Identifies a directly connected network.
- **S** - Identifies a static route created to reach a specific network.
- **O** - Identifies a dynamically learned network from another router using the OSPF routing protocol.
- ***** - This route is a candidate for a default route.

3.5Routing Table entries:

- **Route source:** This identifies how the route was learned.
- **Destination network (prefix and prefix length):** This identifies the address of the remote network.

CamScanner

- **Administrative distance:** This identifies the trustworthiness of the route source. Lower values indicate preferred route source.
- **Metric:** This identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
- **Next-hop**: This identifies the IP address of the next router to which the packet would be forwarded.
- **Route timestamp:** This identifies how much time has passed since the route was learned.
- **Exit interface:** This identifies the egress interface to use for outgoing packets to reach their final destination.

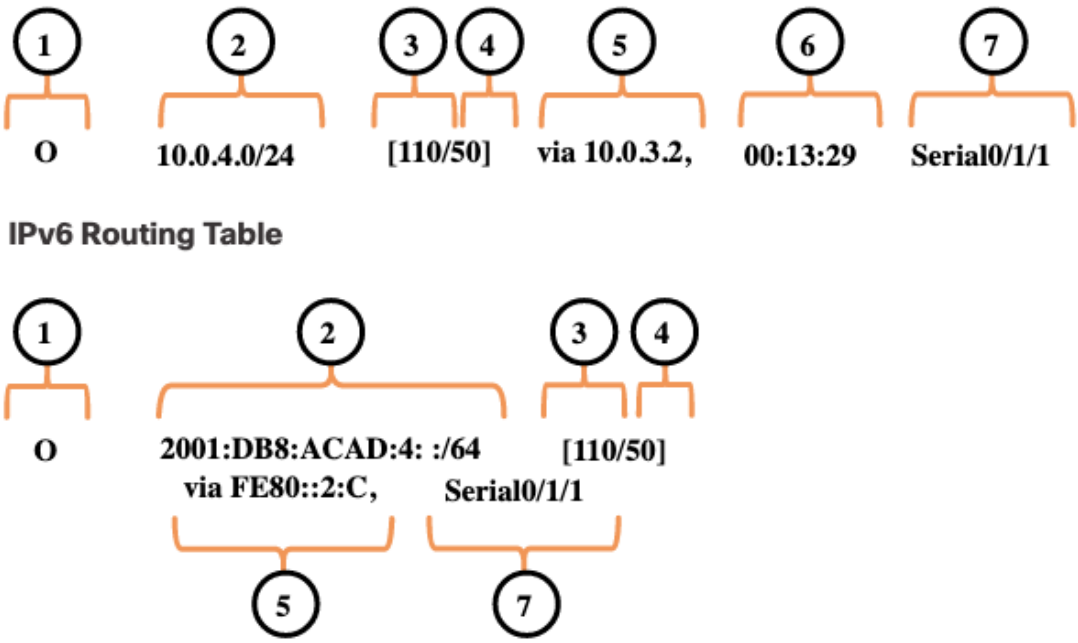


Figure 3.4Routing table entries

CamScanner

3.5.1Directly connected networks

A directly connected network is denoted by a status code of C in the routing table. The route contains a network prefix and prefix length. The routing table also contains a local route for each of its directly connected networks, indicated by the status code of L.

For IPv4 local routes the prefix length is /32 and for IPv6 local routes the prefix length is /128. This means the destination IP address of the packet must match all the bits in the local route for this route to be a match.

The purpose of the local route is to efficiently determine when it receives a packet for the interface instead of a packet that needs to be forwarded.

3.5.2Static routes in IP Routing Protocol

The topology in the figure is simplified to show only one LAN attached to each router.

The figure shows IPv4 and IPv6 static routes configured on R1 to reach the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks on R2.

Static routes do not advertise their presence on the network like dynamic routing protocols, making them less susceptible to attacks that exploit routing protocols.

CamScanner

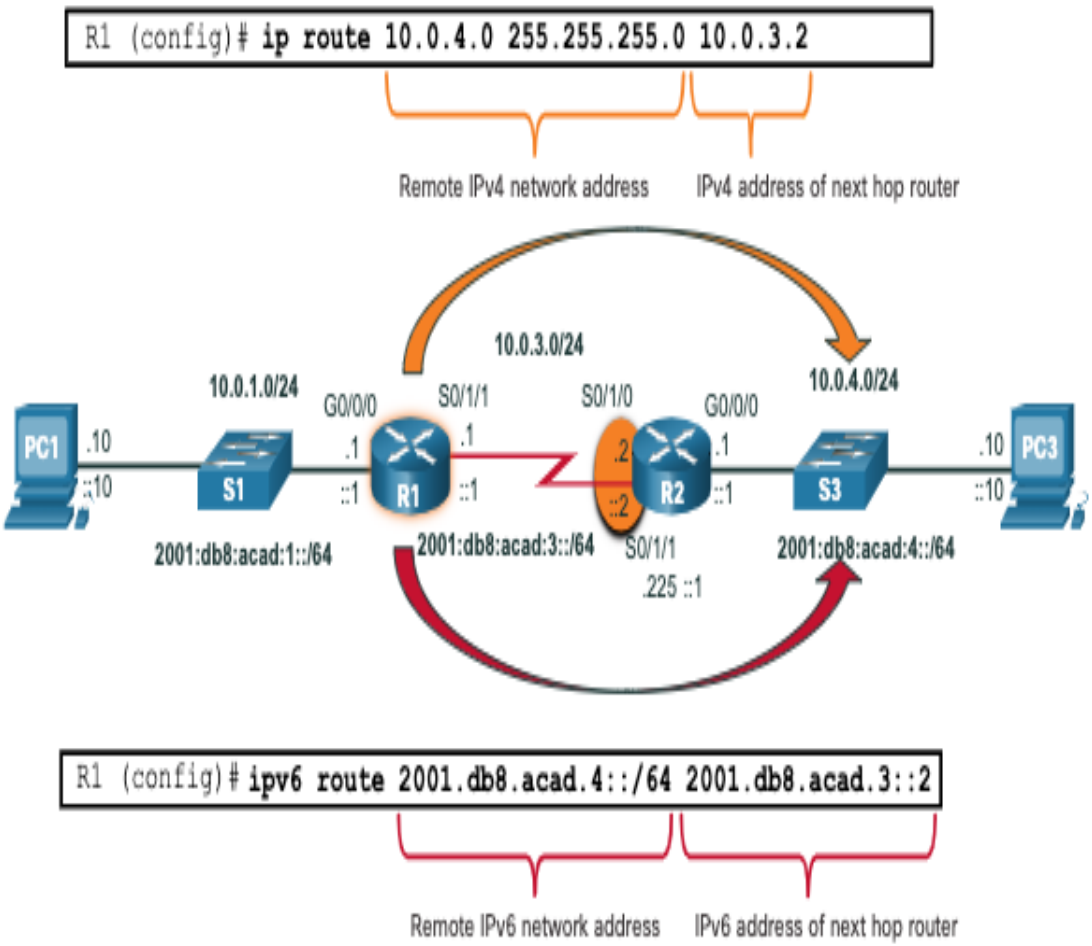


Figure 3.5Static Route

3.6Comparing Dynamic Routing Protocol

CamScanner

Features:

Routers add IP routes to their routing tables using three methods: connected routes, static routes, and routes learned by using dynamic routing protocols.

- **Routing protocol:** A set of messages, rules, and algorithms used by routers for the overall purpose of learning routes. This process includes the exchange and analysis of routing information. Each router chooses the best route to each subnet (path selection) and finally places those best routes in its IP routing table. Examples include RIP, EIGRP, OSPF, and BGP.
- **Routed protocol and routable protocol:** Both terms refer to a protocol that defines a packet structure and logical addressing, allowing routers to forward or route the packets. Routers forward packets defined by routed and routable protocols. Examples include IP Version 4 (IPv4) and IP Version 6 (IPv6).

3.6.1 Interior and Exterior Routing Protocols:

IP routing_protocols fall into one of two major categories: *interior gateway protocols* (IGP) or *exterior gateway protocols* (EGP). The definitions of each are as follows:

- **IGP**: A routing protocol that was designed and intended for use inside a single autonomous system (AS)

CamScanner

- **EGP**: A routing protocol that was designed and intended for use between different autonomous systems

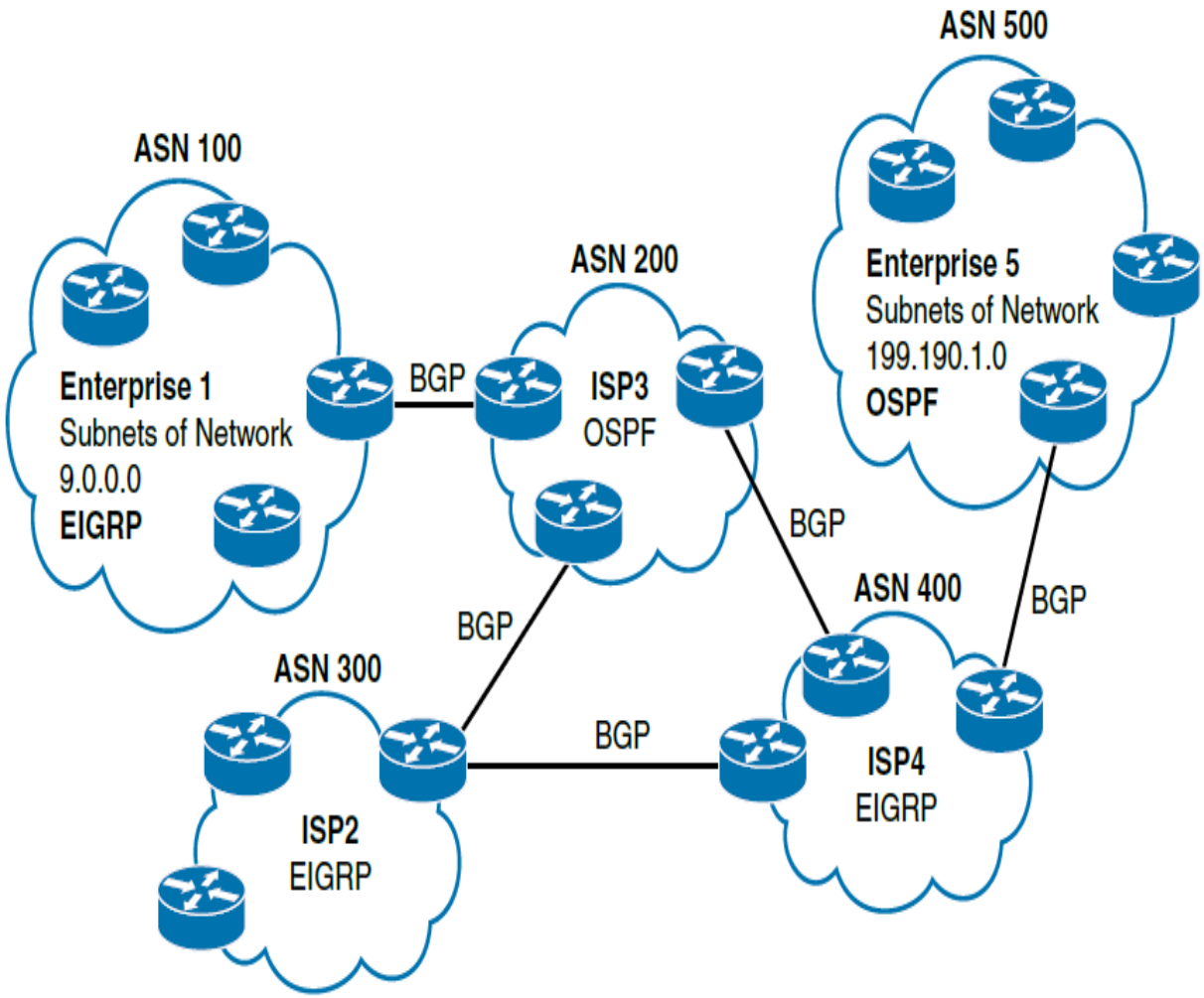


Figure 3.6 Autonomous Systems

CamScanner

3.7OSPF (open shortest path first):

A (link-state) protocol has been used in network to determine the most efficient path for data transmission. It functions by sharing a map of the network topology among all routers, enabling them to calculate the shortest path to any destination.

3.7.1 OSPF FUNDAMENTALS:

- OSPF sends to neighboring routers link-state advertisements (LSAs) that contain the link state and link metric.
- The received LSAs are stored in a local database called the link-state database (LSDB), and they are flooded throughout the OSPF routing domain, just as the advertising router advertised them. All OSPF routers maintain a synchronized identical copy of the LSDB for the same area.
- The LSDB provides the topology of the network, in essence providing for the router a complete map of the network. All OSPF routers run the Dijkstra shortest path first (SPF) algorithm to construct a loop-free topology of shortest paths.
- OSPF dynamically detects topology changes within the network and calculates loop-free paths in a short amount of time with minimal routing protocol traffic
- Each router sees itself as the root or top of the SPF tree (SPT), and the SPT contains all network destinations within the OSPF domain. The SPT differs for each OSPF router.

CamScanner

3.7.2 OSPF Neighbor States:

- Down: This is the initial state of a neighbor relationship. It indicates that the router has not received any OSPF hello packets.
- Attempt: This state is relevant to NBMA networks that do not support broadcast and require explicit neighbor configuration. This state indicates that no information has been received recently, but the router is still attempting communication.
- Initial: This state indicates that a hello packet has been received from another router, but bidirectional communication has not been established.
- 2_way: Bidirectional communication has been established. If a DR or BDR is needed, the election occurs during this state.
- Exstart: This is the first state in forming an adjacency. Routers identify which router will be the master or slave for the LSDB synchronization.
- Exchange: During this state, routers are exchanging link states by using DBD packets.
- Loading: LSR packets are sent to the neighbor, asking for the more recent LSAs that have been discovered (but not received) in the Exchange state.
- Full: Neighboring routers are fully adjacent.

CamScanner

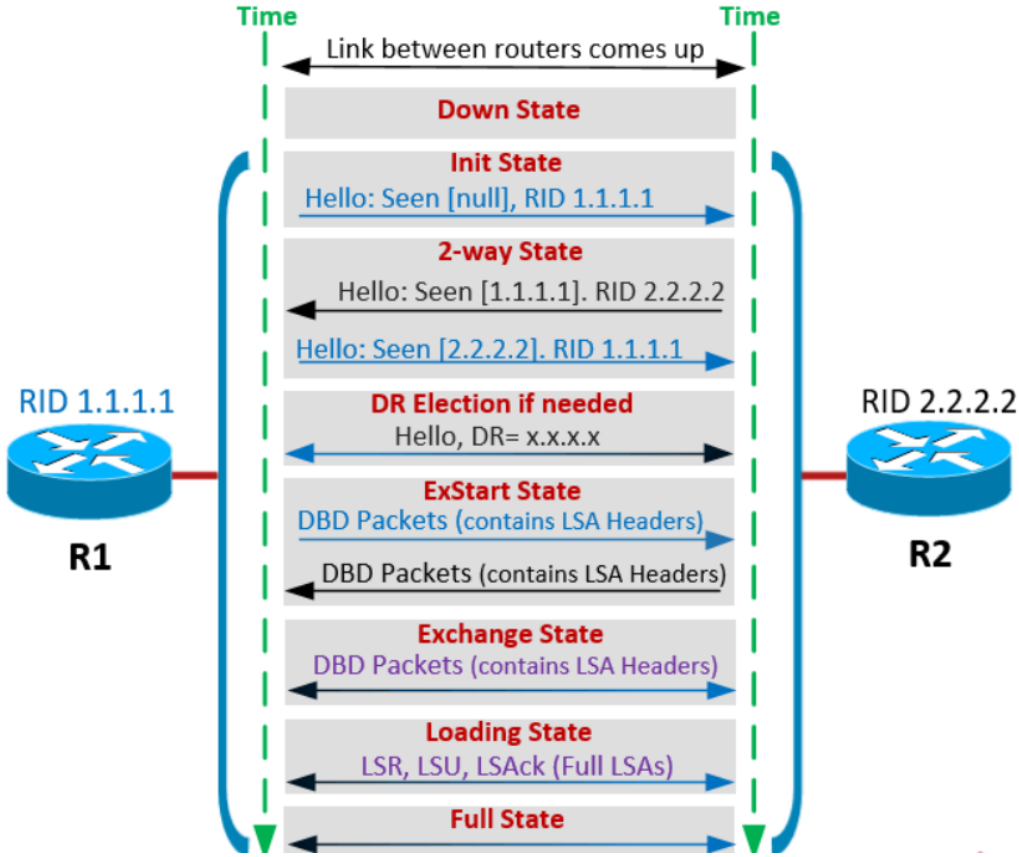


Figure 3.7 OSPF state

3.7.3 Hello Timer:

Changing the hello timer interval modifies the default dead interval, too. The OSPF hello timer is modified with the interface configuration sub mode command ip ospf hello-interval *1–65535, default hello is 10s.*

CamScanner

3.7.4 Dead Interval Timer:

The OSPF dead interval timer can be changed with the command IP OSPF dead interval *1–65535 under the interface configuration sub* mode, default dead id 40s

3.7.5 Area Concept

- An OSPF area is a logical grouping of routers or, more specifically, a logical grouping of router interfaces.
- Area membership is set at the interface level, and the area ID is included in the OSPF hello packet.
- An interface can belong to only one area. All routers within the same
- OSPF area processes an identical copy of the link-state database (LSDB).
- An OSPF area grows in size as network links and number of the routers increase in the area. While using a single area simplifies the topology, there are trade-offs:
- Full shortest path first (SPF) tree calculation runs when a link flaps within the area.
- The LSDB increases in size and becomes unmanageable.
- The LSDB for the area grows, consuming more memory, and taking longer during the SPF computation process.
- No summarization of route information occurs.
- Area 0 is a special area called *the backbone. By design,* all areas must connect to Area 0 because OSPF expects all areas to inject routing

CamScanner

information into the backbone, and Area 0 advertises the routes into other areas.

- *Area border routers (ABRs) are OSPF routers connected* to Area 0 and another OSPF area
- Every ABR needs to participate in Area 0; otherwise, routes will not advertise into another area.

3.7.6 OSPF Multi-Area Topology &Sample Multi-Area OSPF Configuration:

OSPF supports both clear-text and MD5 authentication, adding an extra layer of security to the routing process. OSPF provides a clear view of the network topology, allowing administrators to understand and manage routing paths effectively.

Multi-area OSPF is crucial for scalability and reducing the impact of network changes in large, complex networks. By dividing the network into smaller, more manageable areas, it minimizes routing table sizes, limits the propagation of topology changes, and optimizes routing calculations, enhancing network stability and performance.

Multi-area OSPF allows routers to only maintain detailed information about their specific area and summarized information about other areas. This reduces the size of routing tables, making them more manageable and improving routing efficiency.

CamScanner

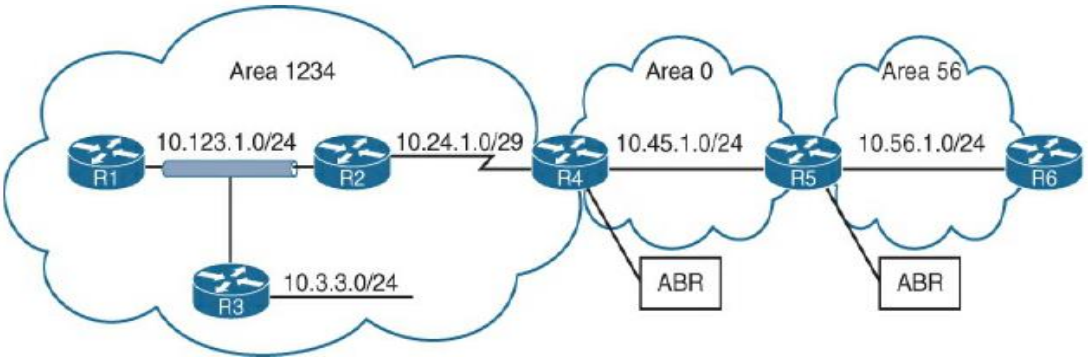


Figure 3.8 OSPF Multi-area

```
R4
router ospf 1
 router-id 192.168.4.4
 network 10.24.1.0 0.0.0.255 area 1234
 network 10.45.1.0 0.0.0.255 area 0
```

Figure 3.9 Area Configuration

3.7.7 LSA Types:

All routers within an OSPF area have an identical set of LSAs for that area. The ABRs maintain a separate set of .LSAs for each OSPF area. Most LSAs in one area will be different from the LSAs in another area.

3.7.7.1 LSA Type 1: Router Link

CamScanner

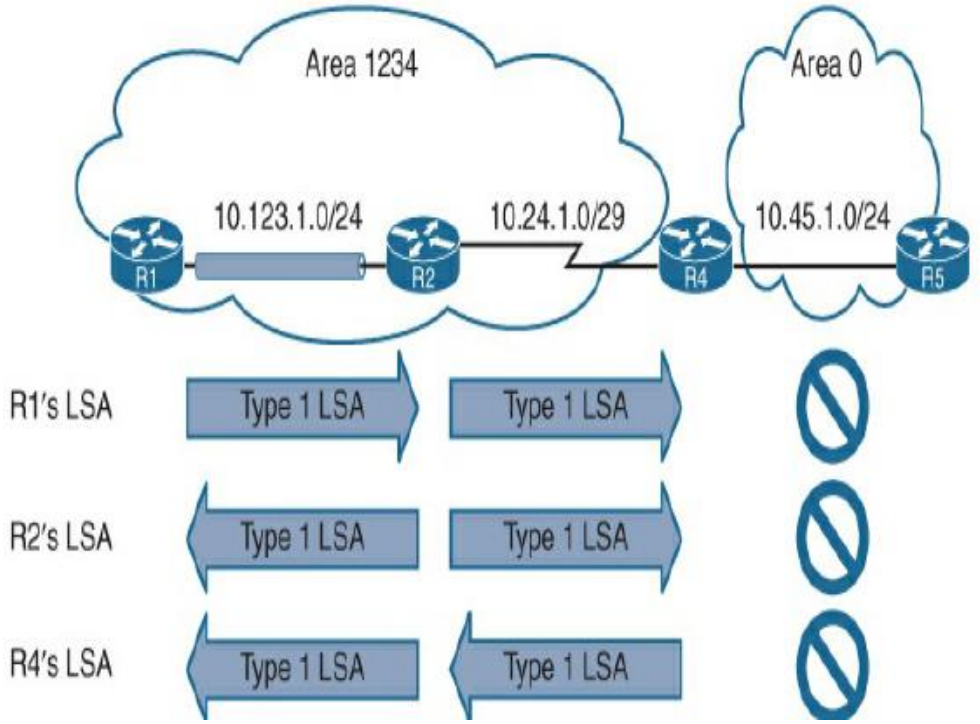


Figure 3.10 LAS type 1

3.7.7.2 LSA Type 2: Network Link

- A type 2 LSA represents a multi-access network segment that uses a DR. The DR always advertises the type 2 LSA and identifies all the routers attached to that network segment.
- Like type 1 LSAs, Type 2 LSAs are not flooded outside the originating OSPF area.
- Detailed type 2 LSA information is shown with the command show IP OSPF database network.

CamScanner

3.7.7.3LSA Type 3: Summary Link

- When an ABR receives a type 1 LSA, it creates a type 3 LSA referencing the network in the original type 1 LSA; the type 2 LSA is used to determine the network mask of the multi-access network.
- The ABR then advertises the type 3 LSA into other areas.
- If an ABR receives a type 3 LSA from Area 0 (the backbone), it regenerates a new type 3 LSA for the Non back bone area and lists itself as the advertising router, with the additional cost metric.[12]

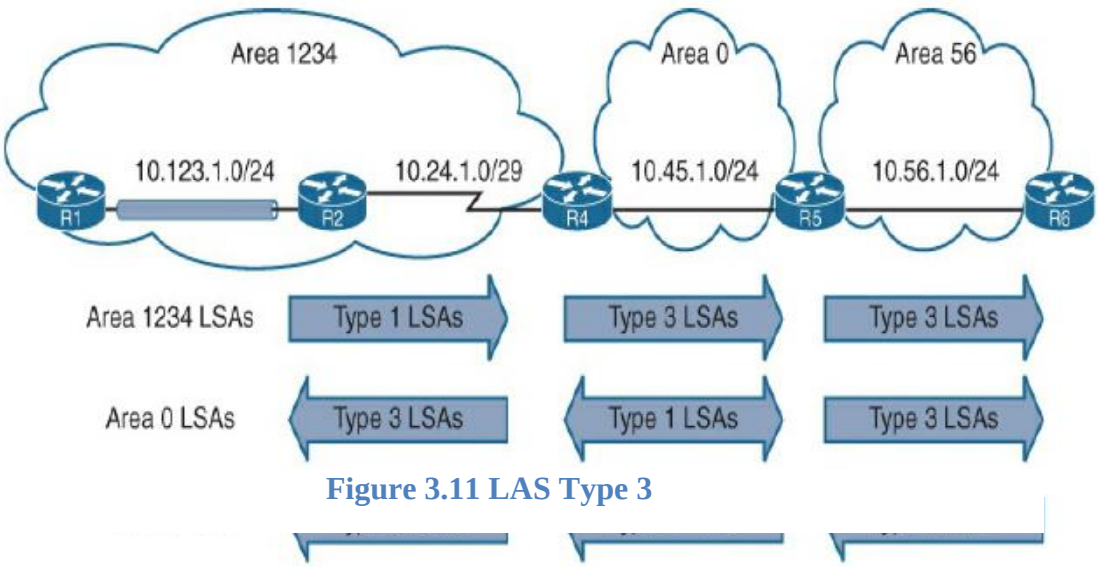


Figure 3.11 LAS Type 3

CamScanner

3.8 Routing Filtering

3.8.1 Filtering with Summarization

- One of the easiest methodologies for filtering routes is to use the not-advertise keyword during prefix summarization.
- Using this keyword prevents creation of any type 3 LSAs for any networks in that range, thus making the subordinate routes visible only within the area where the route originates.
- The full command structure is area *area-id range network subnet-mask not-advertise under the OSPF* process.

3.8.2 Area Filtering:

Area *area-id filter-list prefix prefix-list name* {in | out} in ABR

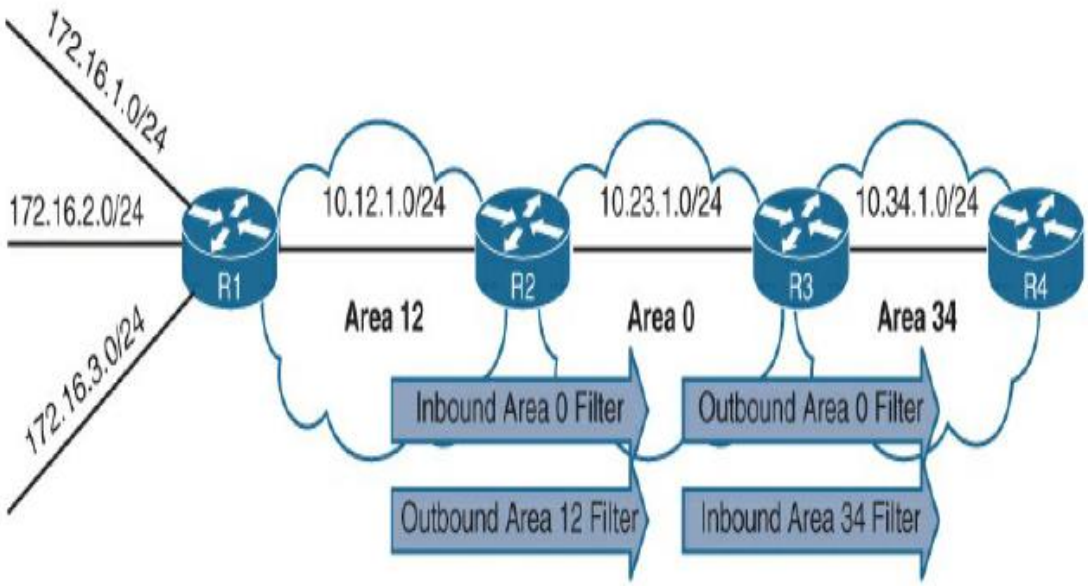


Figure 3.12 Area Filtering

CamScanner

3.9 EIGRP (Enhanced Interior Gateway Protocol)

- EIGRP overcomes the deficiencies of other distance vector routing protocols like RIP with features such as unequal-cost load balancing, support for networks 255 hops away, and rapid convergence features.
- EIGRP uses a diffusing update algorithm (DUAL) to identify network paths and enable fast convergence using pre calculated loop-free backup paths.

3.9.1EIGRP Topology Table:

```
R1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.12.1.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/3
P 10.13.1.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/1
P 10.14.1.0/24, 1 successors, FD is 5120
        via Connected, GigabitEthernet0/2
P 10.23.1.0/24, 2 successors, FD is 3072
        via 10.12.1.2 (3072/2816), GigabitEthernet0/3
        via 10.13.1.3 (3072/2816), GigabitEthernet0/1
P 10.34.1.0/24, 1 successors, FD is 3072
        via 10.13.1.3 (3072/2816), GigabitEthernet0/1
        via 10.14.1.4 (5376/2816), GigabitEthernet0/2
```

CamScanner

3.9.2EIGRP path:

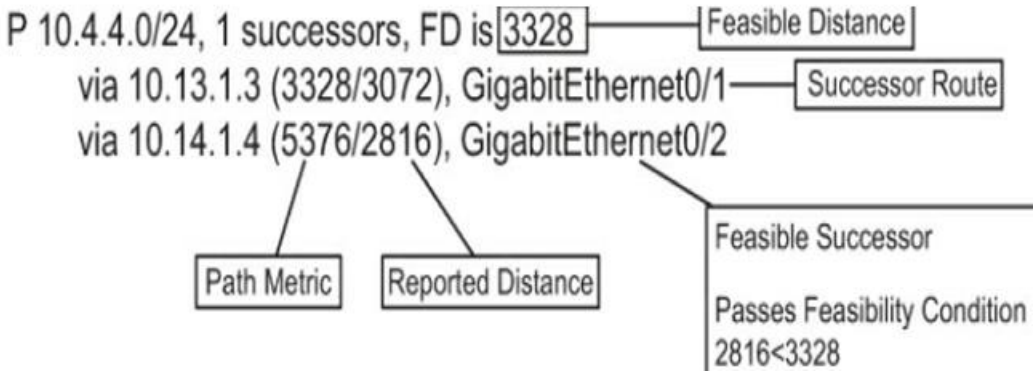


Figure 3.14 EIGRP path

3.9.3 EIGRP Neighbors:

- EIGRP neighbors exchange the entire routing table when forming an adjacency, and they advertise only incremental updates as topology changes occur within a network.
- The neighbor adjacency table is vital for tracking neighbor status and the updates sent to each neighbor.
- It uses multicast packets where possible and unicast packets when necessary.
- Communication between routers is done with multicast, using the group address 224.0.0.10

3.9.4 Convergence:

When EIGRP detects that it has lost its successor for a path, the feasible successor instantly becomes the successor route, providing a backup route.

CamScanner

3.9.4.1 EIGRP Convergence Topology:

- The following steps are processed in order from the perspective of R2 calculating a new route to the 10.1.1.0/24 network:
- Step 1. R2 detects the link failure. R2 does not have a feasible successor for the route, sets the 10.1.1.0/24 prefix as active, and sends queries to R3 and R4.
- Step 2. R3 receives the query from R2 and processes the Delay field that is set to infinity. R3 does not have any other EIGRP neighbors and sends a reply to R2 saying that a route does not exists. R4 receives the query from R2 and processes the Delay field that is set to infinity. Because the query was received by the successor, and a feasible successor for the prefix does not exist, R4 marks the route as active and sends a query to R5.
- Step 3. R5 receives the query from R4.
- Query was received by a Non successor and a successor exists on a different interface, a reply for the 10.4.4.0/24 network is sent back to R2 with the appropriate EIGRP attributes.
- Step 4. R4 receives R5's reply, acknowledges the packet, and computes a new path. Because this is the last outstanding query packet on R4, R4 sets the prefix as passive. With all queries satisfied, R4 responds to R2's query with the new EIGRP metrics.
- Step 5. R2 receives R4's reply, acknowledges the packet, and computes a new path. Because this is the last outstanding query packet on R4, R2 sets the prefix as passive.

CamScanner

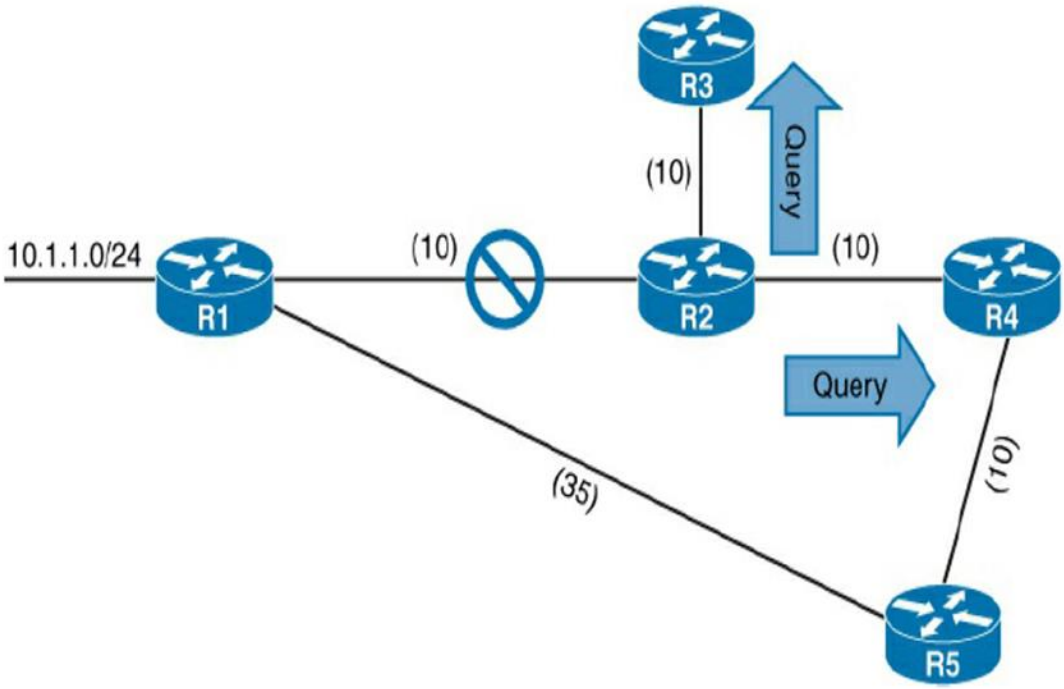


Figure 3.15 EIGRP Query

3.9.5 Redistribution between EIGRP and OSPF

- R1 and R2 run EIGRP.
- R2 and R3 run OSPF.

R2 will redistribute between OSPF and EIGRP. Once that's done, we should be able to ping between the loopback interfaces of R1 and R3.

The configuration of EIGRP between R1 and R2:

R1 (config) #router eigrp 12

R1 (config-router) #no auto-summary

CamScanner

R1 (config-router) #network 1.1.1.1 0.0.0.0

R1 (config-router) #network 192.168.12.0

R2 (config) #router eigrp 12

R2 (config-router) #no auto-summary

R2 (config-router) #network 192.168.12.0

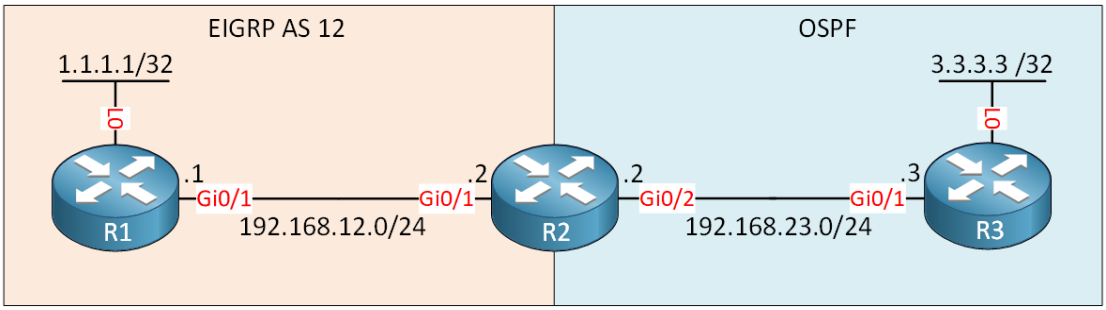


Figure 3.16 Redistribution

And let's configure OSPF between R2 and R3:

R2 (config) #router ospf 1

R2 (config-router)#network 192.168.23.0 0.0.0.255 area 0

R3 (config) #router ospf 1

R3 (config-router) #network 192.168.23.0 0.0.0.255 area 0

R3 (config-router) #network 3.3.3.3 0.0.0.0 area 0

R2 sees R1 as an EIGRP neighbor and R3 as an OSPF neighbor.

CamScanner

R2#**show IP route**

1.0.0.0/32 is subnetted, 1 subnets

D 1.1.1.1 [90/130816] via 192.168.12.1, 00:42:39, GigabitEthernet0/1

3.0.0.0/32 is subnetted, 1 subnets

O 3.3.3.3 [110/2] via 192.168.23.3, 00:41:25, GigabitEthernet0/2

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.12.0/24 is directly connected, GigabitEthernet0/1

L 192.168.12.2/32 is directly connected, GigabitEthernet0/1

192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.23.0/24 is directly connected, GigabitEthernet0/2

L 192.168.23.2/32 is directly connected, GigabitEthernet0/2

Redistribute OSPF into EIGRP:

First, we'll redistribute OSPF into EIGRP. We do this under the EIGRP process:

R2 (config) #router eigrp 12

Let's take a look at the redistribute ospf options:

R2 (config-router) #redistribute ospf ?

<1-65535> Process ID

CamScanner

We need to select the correct OSPF process. In our example, that's process ID 1. There are three options you can choose from:

R2 (config-router)#redistribute ospf 1 ?

Match: Redistribution of OSPF routes

Metric: Metric for redistributed routes

Route-map: Route map reference

With the match option, we can choose to redistribute only specific OSPF routes like external or internal routes. The route-map is another option only to redistribute specific OSPF routes, for example, by using an access-list.

We'll keep it simple for now and just redistribute all OSPF routes into EIGRP. We have to specify a metric, if we don't, redistribution fails.

EIGRP and OSPF use different metrics and there is no way to convert from one metric to another. This means we have to configure the metric ourselves.[13]

CamScanner

CamScanner

1-project Overview

The project simulates an enterprise network infrastructure that interconnects 9 fully meshed branches using the OSPF routing protocol.

2-Project concept

The project represents a comprehensive enterprise infrastructure that interconnects 9 distinct branches through dynamic routing. It is designed to ensure high connectivity efficiency, optimized traffic engineering,and robust fault management.

3-Implementation details

Dynamic routing: interconnecting all 9 branches using OSPF routing to achieve high routing efficiency.

Departmental segmentation:Dividing the 1st and 2nd branches into multiple departments(VLANS)and routing them to form a unified local network.

Data center & call center:Designing the 3rd branch to host the central data center and call center and connect with all other branches.

VOIP system Implementation:to connect all ip phones across all branches under a single corporate voice system.

wireless infrastructure:Building the 4th branch as a fully wireless network environment (WLAN).

IPV6 addressing: Implementing IPV6 addressing and routing within the 5th and 6th branches

Layer 3 Switching:using layer 3 switch as core devices alongside Routers in the 7th and 8th branches.

EtherChannel & Load Balancing:Designing the 9th branch using Etherchannel technology to achieve link aggregation,load balancing,and minimal propagation delay.

4-protocols

1-ospf(open shortest path first)

2-VLAN(virtual local area network IEEE 802.1Q) it is used to segment the central switch ,isolating each department (e.g.,HR,IT,Planning) into a separate virtual network .

3-DHCP(Dynamic Host configuration protocol)

4-RIP

CamScanner

The first and second branch:

GATEWAY	SUBNET MASK	SUBNET ID	VLAN NAME	NUMBER OF VLAN	BRANCH
192.168.10.1	255.255.255.240	192.168.10.0/28	HR	VLAN 10	Branch 1
192.168.20.1	255.255.255.240	192.168.20.0/28	Sales	VLAN 20	
192.168.30.1	255.255.255.240	192.168.30.0/28	marketing	VLAN 30	
192.168.40.1	255.255.255.240	192.168.40.0/28	maneger	VLAN 40	
192.168.50.1	255.255.255.240	192.168.50.0/28	PR(Public relations)	VLAN 50	
192.168.60.1	255.255.255.240	192.168.60.0/28	planning	VLAN 60	
192.168.70.1	255.255.255.240	192.168.70.0/28	Quality	VLAN 70	
192.168.80.1	255.255.255.240	192.168.80.0/28	CEO	VLAN 80	
192.168.90.1	255.255.255.240	192.168.90.0/28	Call center	VLAN 90	
192.168.100.1	255.255.255.240	192.168.100.0/28	Admin	VLAN 100	
192.168.110.1	255.255.255.240	192.168.110.0/28	engineering	VLAN 110	
192.168.120.1	255.255.255.192	192.168.120.0/28	voip(Voice date)	VLAN 120	
192.168.130.1	255.255.255.240	192.168.130.0/28	servers pool	VLAN 130	
192.168.140.1	255.255.255.240	192.168.140.0/28	Accounting	VLAN 140	Branch 2
192.168.150.1	255.255.255.240	192.168.150.0/28	Engineering	VLAN 150	
192.168.160.1	255.255.255.240	192.168.160.0/28	tech support	VLAN 160	
192.168.170.1	255.255.255.240	192.168.170.0/28	HR(branch 2)	VLAN 170	
192.168.180.1	255.255.255.240	192.168.180.0/28	voip	VLAN 180	

CamScanner

Branch 1;Floor Distribution and core switch AggregatioN

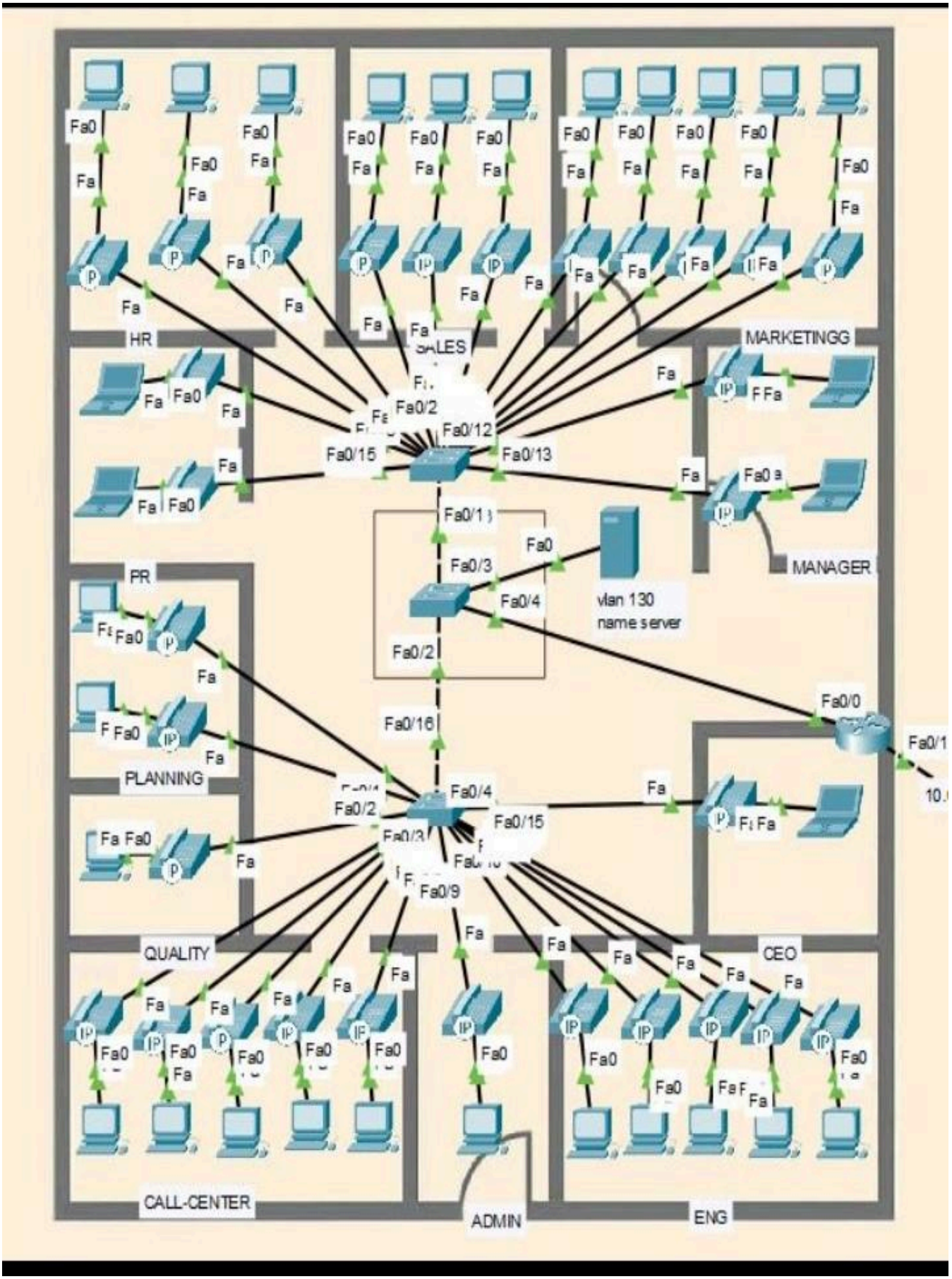
The branch 1 building consists of two floors. The switch access ports on both floors have been configured as multi-VLAN Access port

***Switch B1 floor 1*:VLANs ranging from VLAN 10 TO VLAN 50 have been configured.**

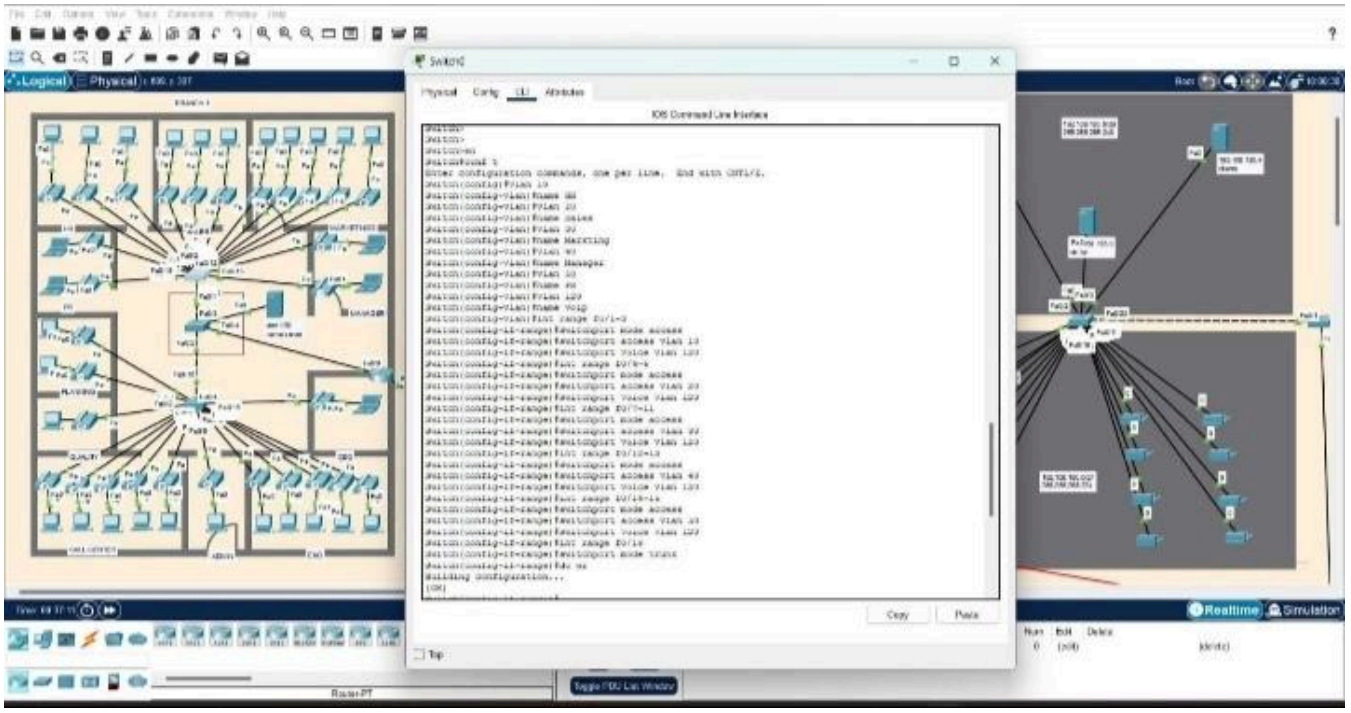
***Switch B1 floor 2*:this switch serves the upper corporate departments (CEO,Planning,call center,quality,Admin,Eng).the range from VLAN 60 TO VLAN 110 has been activated.**

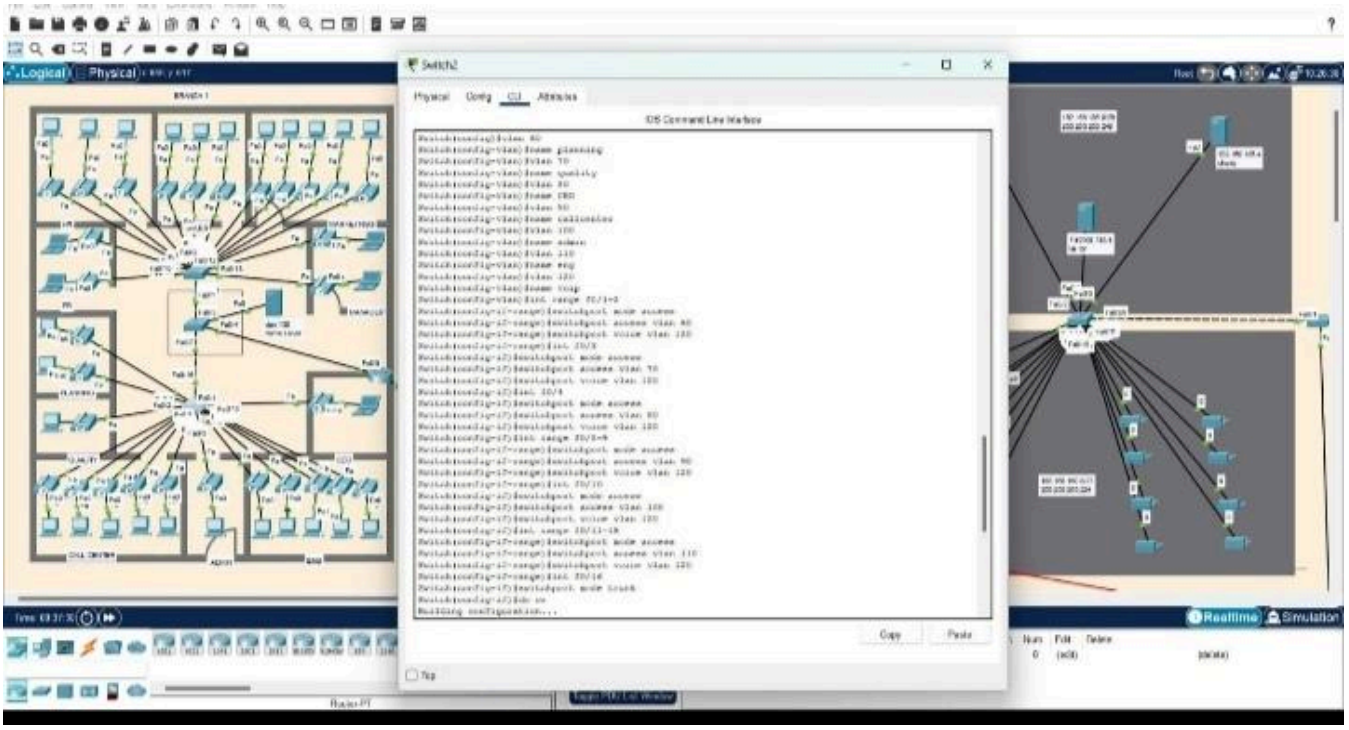
***Switch core B1*:operates as a central aggregation point (Aggregation switch)that receives the incoming trunk links from the floor switches via ports f0/1-2 and f0/4. fo/3 to connecting the server environment within the isolated network range of VLAN 130.**

CamScanner

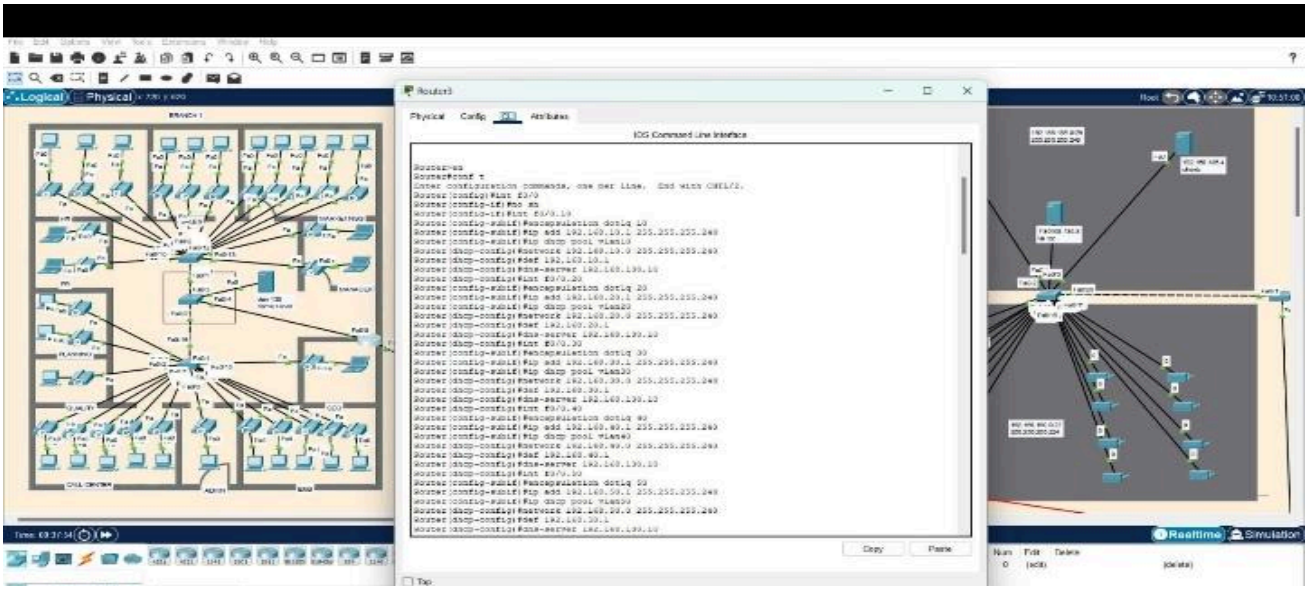

HR
SALES
MARKETINGG
PR
MANAGER
PLANNING
QUALITY
CEO
CALL-CENTER
ADMIN
ENG
vlan 130
name server
Fa0/2
Fa0/12
Fa0/15
Fa0/13
Fa0/3
Fa0/4
Fa0/16
Fa0/9
Fa0/0
Fa0
Fa

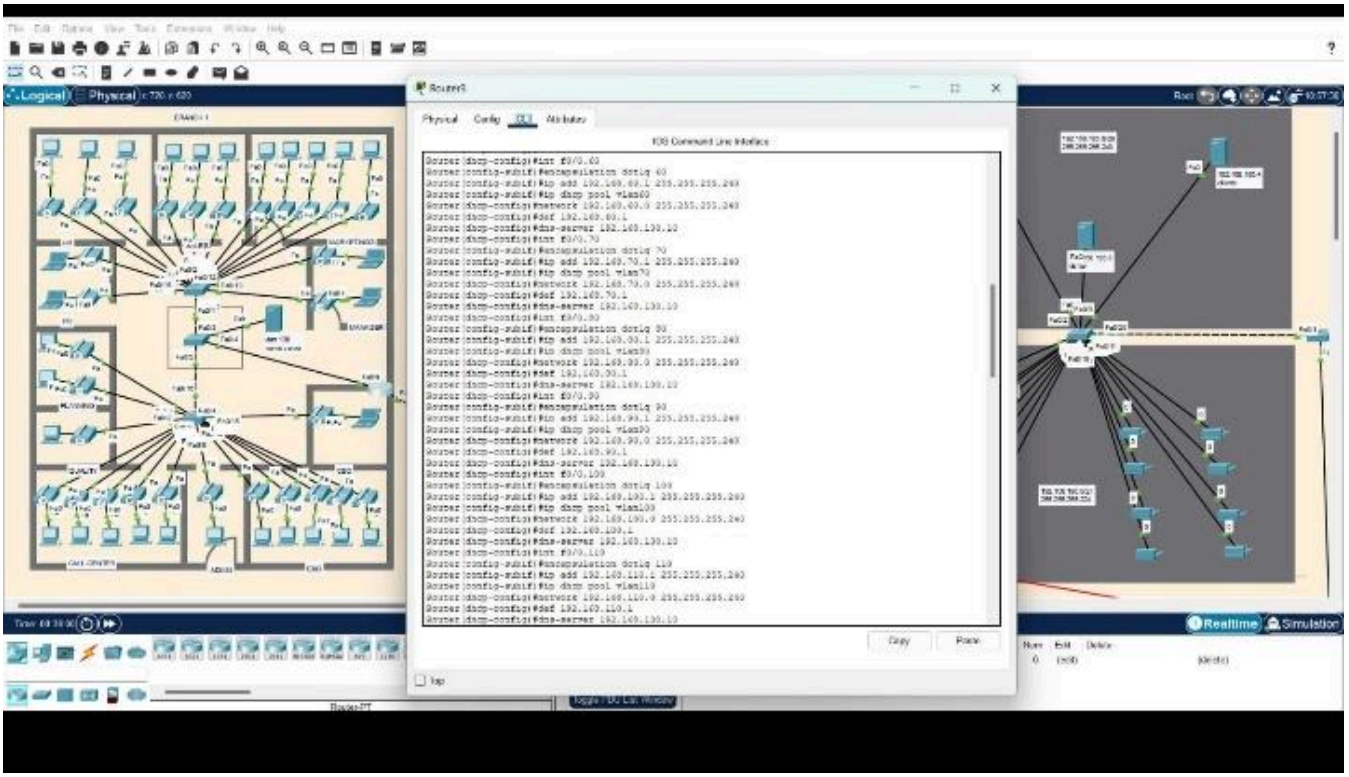
CamScanner





CamScanner





CamScanner

Branch 2:switches and connected Branches infrastructure

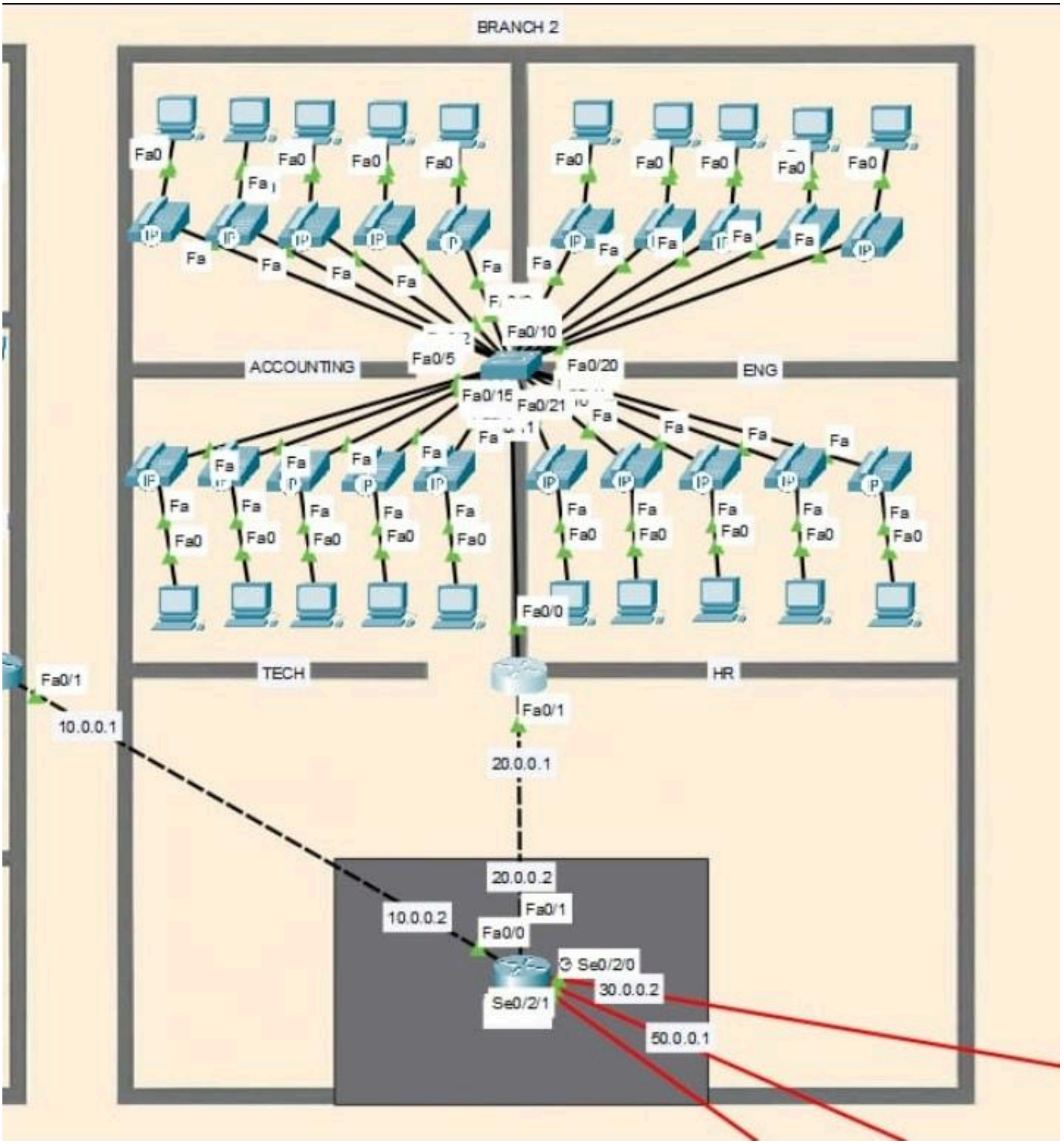
Departmental Structure:the infrastructure of the main switch (switch2)is configured to support 4 independent administrative and technical departments:(HR,Tech,Eng,Accounting)

port Assignment:the physical interfaces from f0/1 to f0/20 are designated and assigned to connect the end devices

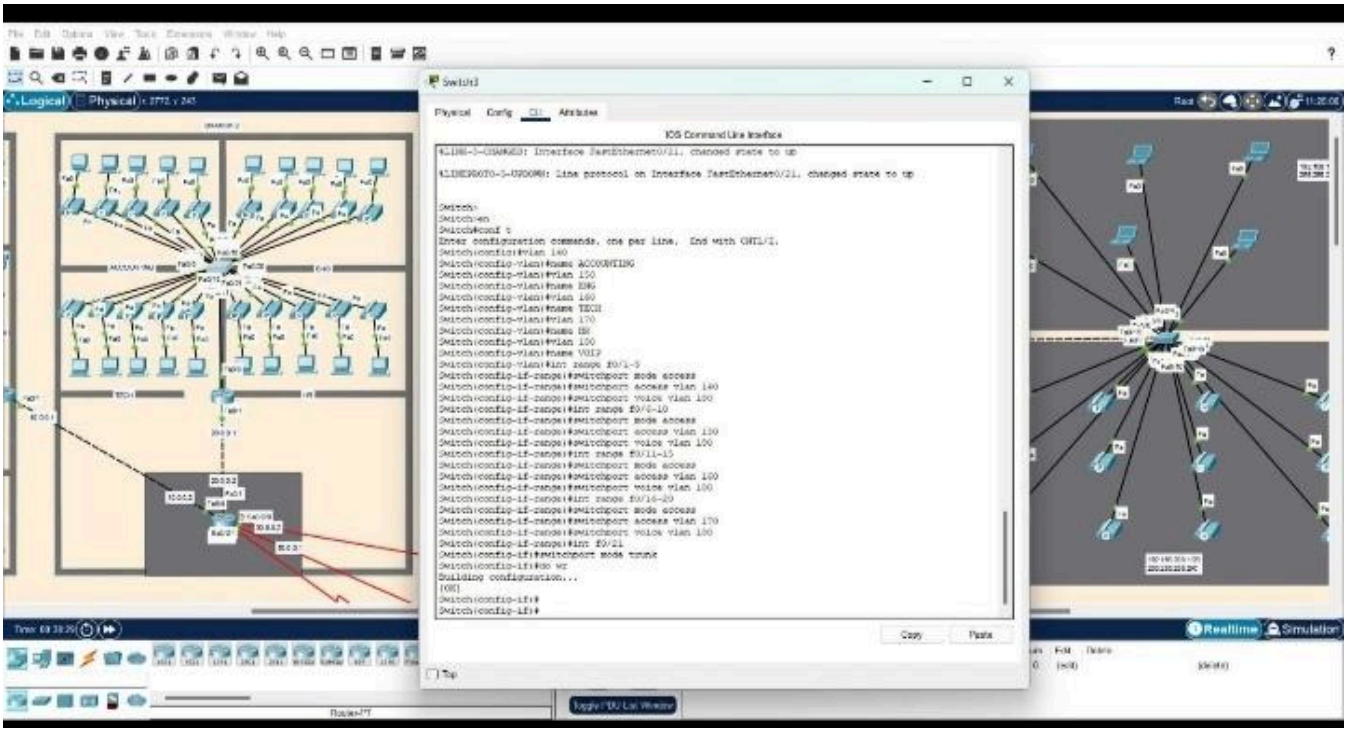
Voice Network(VOIP):A dedicated VLAN 180 is allocated specifically for voice communication services within this branch to ensure high quality,isolated voice traffic separate from regular data.

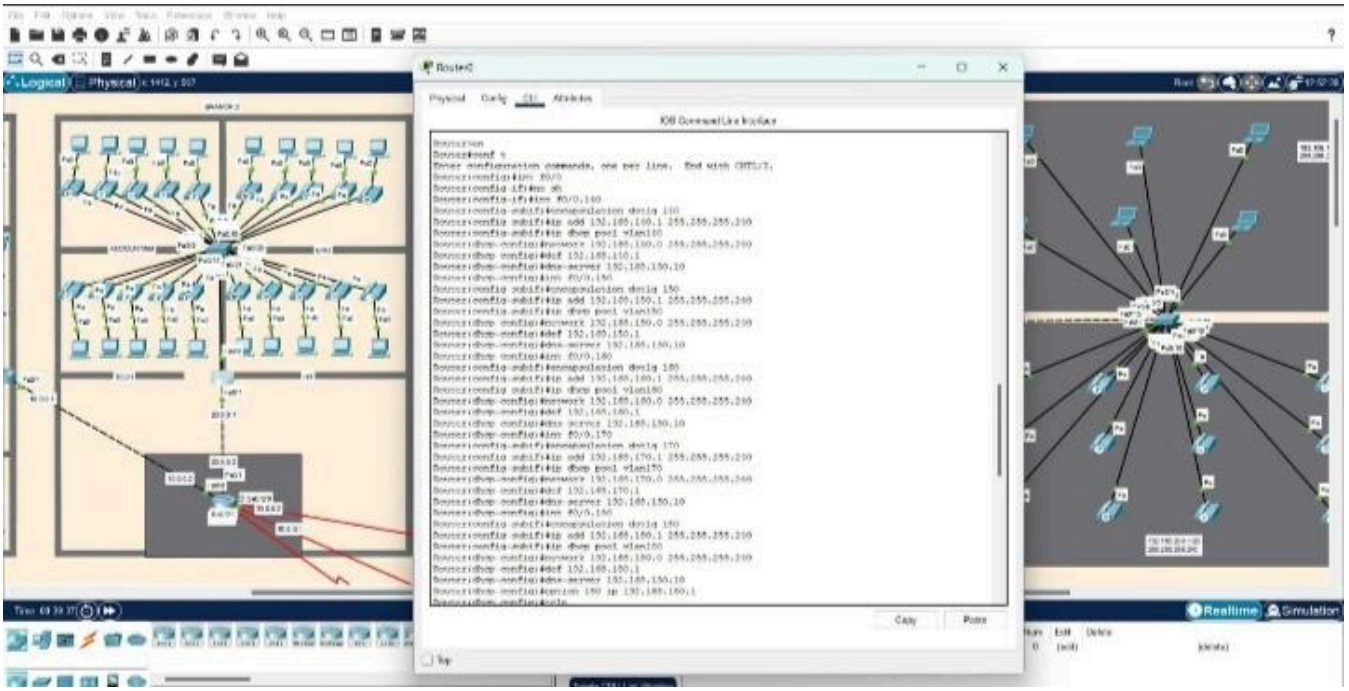
Trunk port:port f0/21 is configured as a trunk line to carry and forward traffic from all different Vlans between the switch and the router.

CamScanner

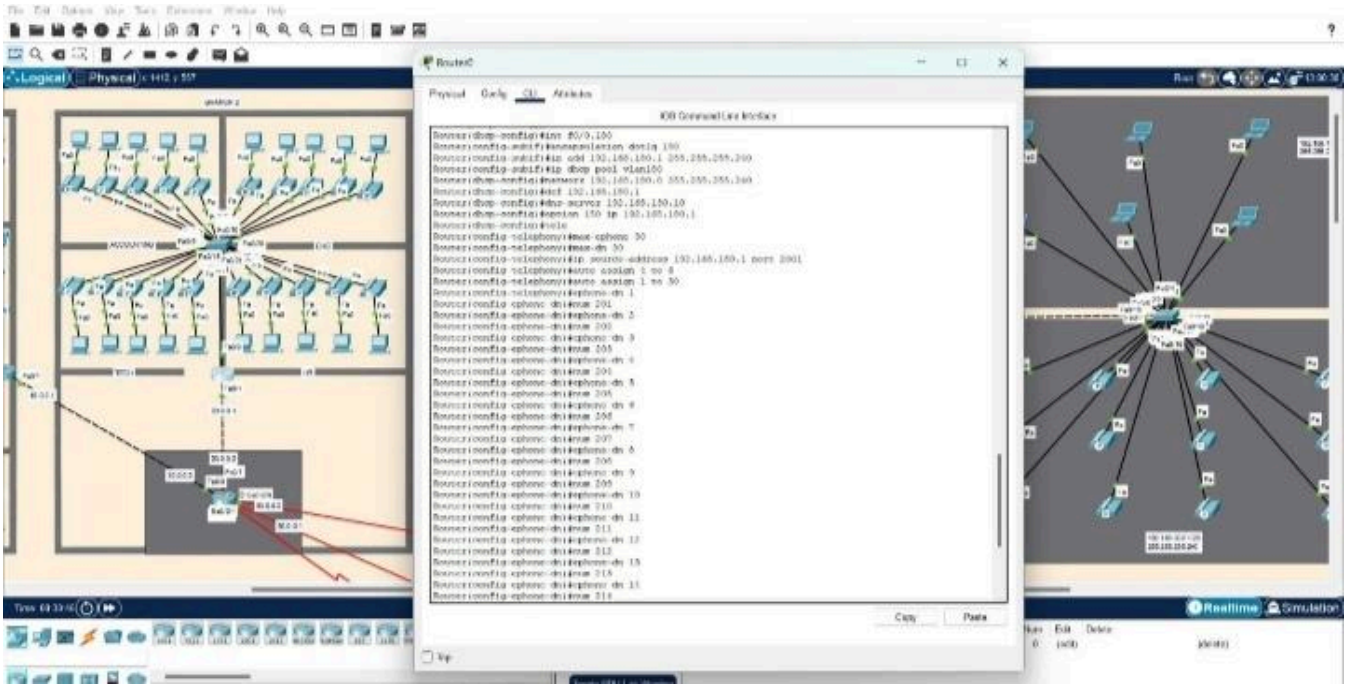

BRANCH 2
ACCOUNTING
ENG
TECH
HR
Fa0/10
Fa0/5
Fa0/20
Fa0/15
Fa0/21
Fa0/0
Fa0/1
10.0.0.1
20.0.0.1
20.0.0.2
10.0.0.2
Se0/2/0
Se0/2/1
30.0.0.2
50.0.0.1

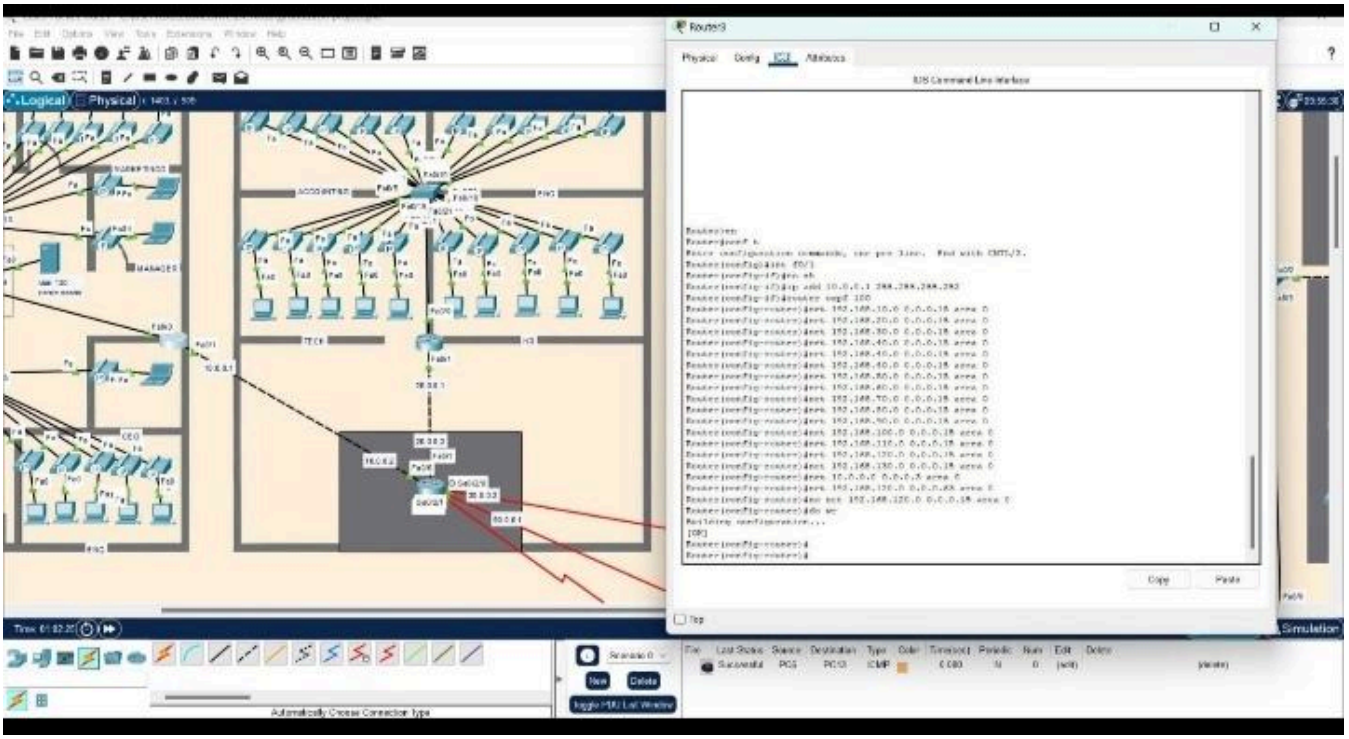
CamScanner


Switch3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 140
Switch(config-vlan)#name ACCOUNTING
Switch(config-vlan)#vlan 150
Switch(config-vlan)#name ENG
Switch(config-vlan)#vlan 160
Switch(config-vlan)#name TECH
Switch(config-vlan)#vlan 170
Switch(config-vlan)#name HR
Switch(config-vlan)#vlan 100
Switch(config-vlan)#name VOIP
Switch(config-vlan)#int range f0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 140
Switch(config-if-range)#switchport voice vlan 100
Switch(config-if-range)#int range f0/6-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 150
Switch(config-if-range)#switchport voice vlan 100
Switch(config-if-range)#int range f0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 160
Switch(config-if-range)#switchport voice vlan 100
Switch(config-if-range)#int range f0/16-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 170
Switch(config-if-range)#switchport voice vlan 100
Switch(config-if-range)#int f0/21
Switch(config-if)#switchport mode trunk
Switch(config-if)#do wr
Building configuration...
[OK]
Switch(config-if)#
Switch(config-if)#
Copy
Paste
Top
Logical
Physical
Realtime
Simulation

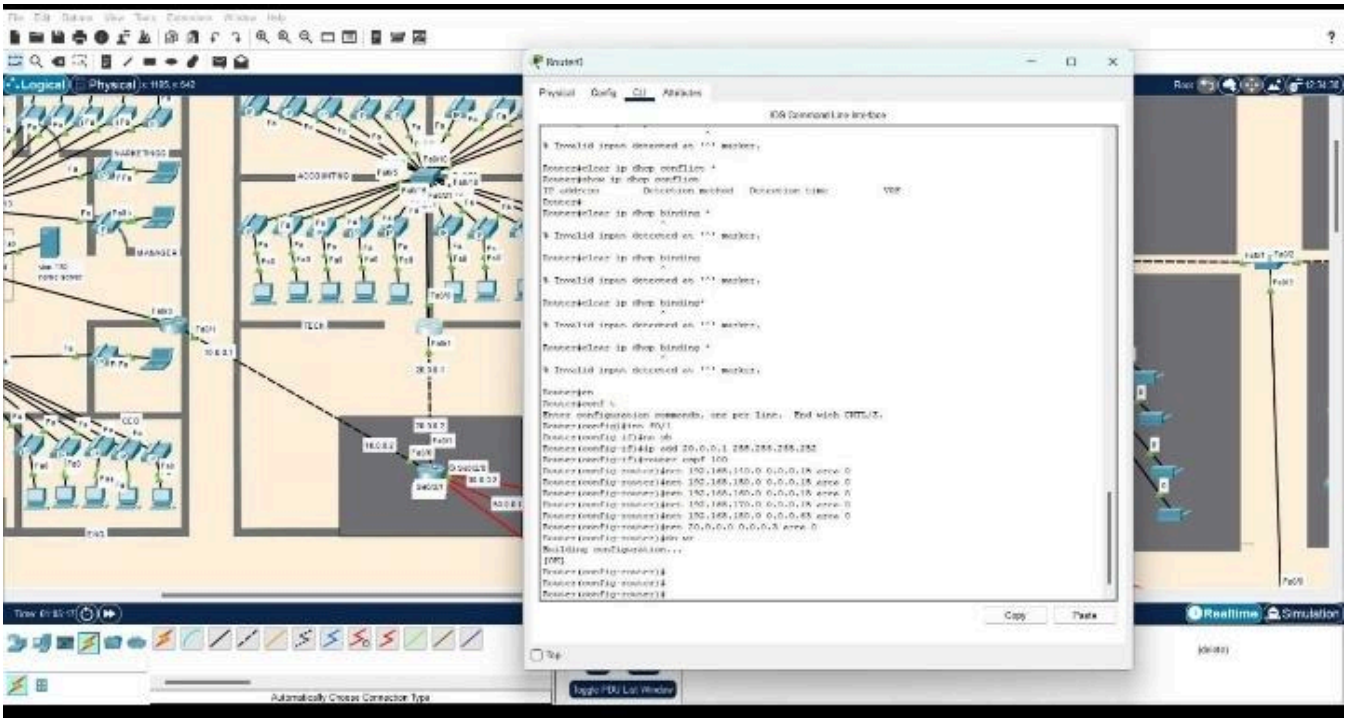

Router2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#no sh
Router(config-if)#int f0/0.140
Router(config-subif)#encapsulation dot1q 140
Router(config-subif)#ip add 192.168.140.1 255.255.255.240
Router(config-subif)#ip dhcp pool vlan140
Router(dhcp-config)#network 192.168.140.0 255.255.255.240
Router(dhcp-config)#def 192.168.150.1
Router(dhcp-config)#dns-server 192.168.150.10
Router(dhcp-config)#int f0/0.150
Router(config-subif)#encapsulation dot1q 150
Router(config-subif)#ip add 192.168.150.1 255.255.255.240
Router(config-subif)#ip dhcp pool vlan150
Router(dhcp-config)#network 192.168.150.0 255.255.255.240
Router(dhcp-config)#def 192.168.150.1
Router(dhcp-config)#dns-server 192.168.150.10
Router(dhcp-config)#int f0/0.160
Router(config-subif)#encapsulation dot1q 160
Router(config-subif)#ip add 192.168.160.1 255.255.255.240
Router(config-subif)#ip dhcp pool vlan160
Router(dhcp-config)#network 192.168.160.0 255.255.255.240
Router(dhcp-config)#def 192.168.150.1
Router(dhcp-config)#dns-server 192.168.150.10
Router(dhcp-config)#int f0/0.170
Router(config-subif)#encapsulation dot1q 170
Router(config-subif)#ip add 192.168.170.1 255.255.255.240
Router(config-subif)#ip dhcp pool vlan170
Router(dhcp-config)#network 192.168.170.0 255.255.255.240
Router(dhcp-config)#def 192.168.170.1
Router(dhcp-config)#dns-server 192.168.150.10
Router(dhcp-config)#int f0/0.160
Router(config-subif)#encapsulation dot1q 160
Router(config-subif)#ip add 192.168.160.1 255.255.255.240
Router(config-subif)#ip dhcp pool vlan160
Router(dhcp-config)#network 192.168.160.0 255.255.255.240
Router(dhcp-config)#def 192.168.150.1
Router(dhcp-config)#dns-server 192.168.150.10
Router(dhcp-config)#exclude 160 ip 192.168.160.1
Copy
Paste
Top
Logical
Physical
Realtime
Simulation

CamScanner

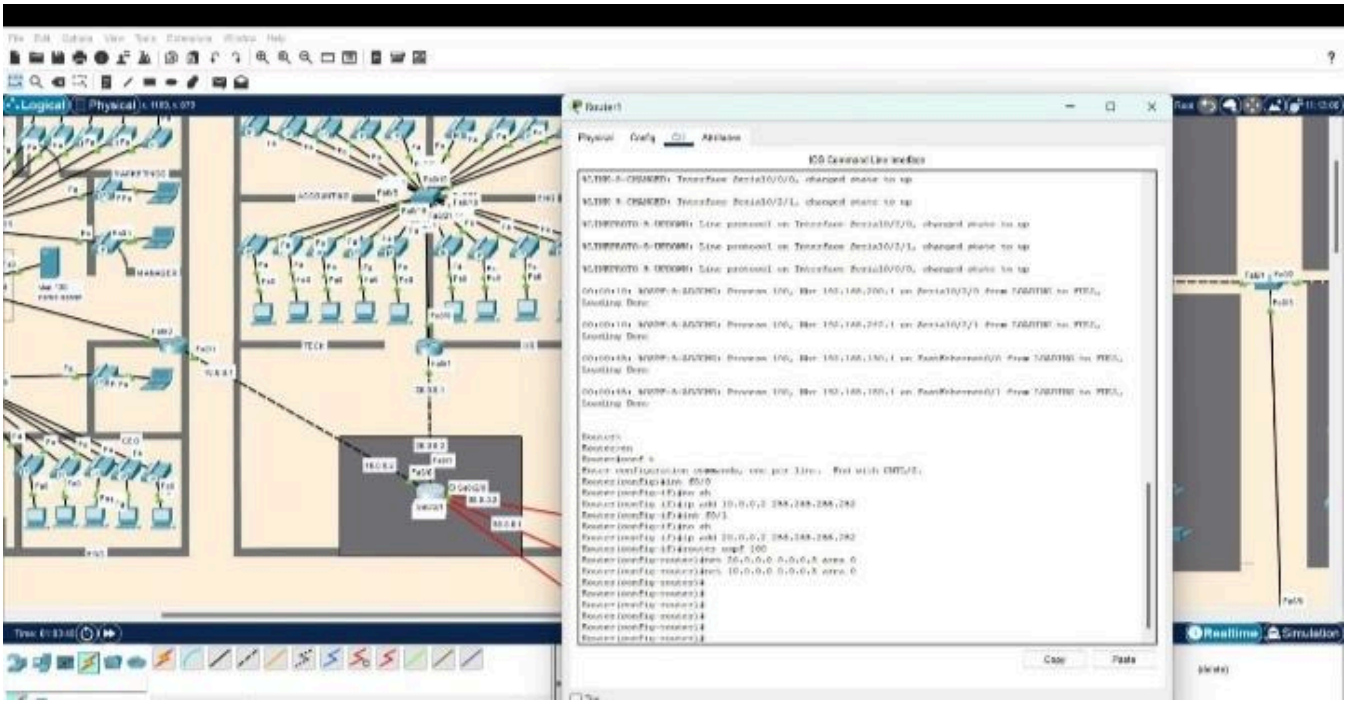


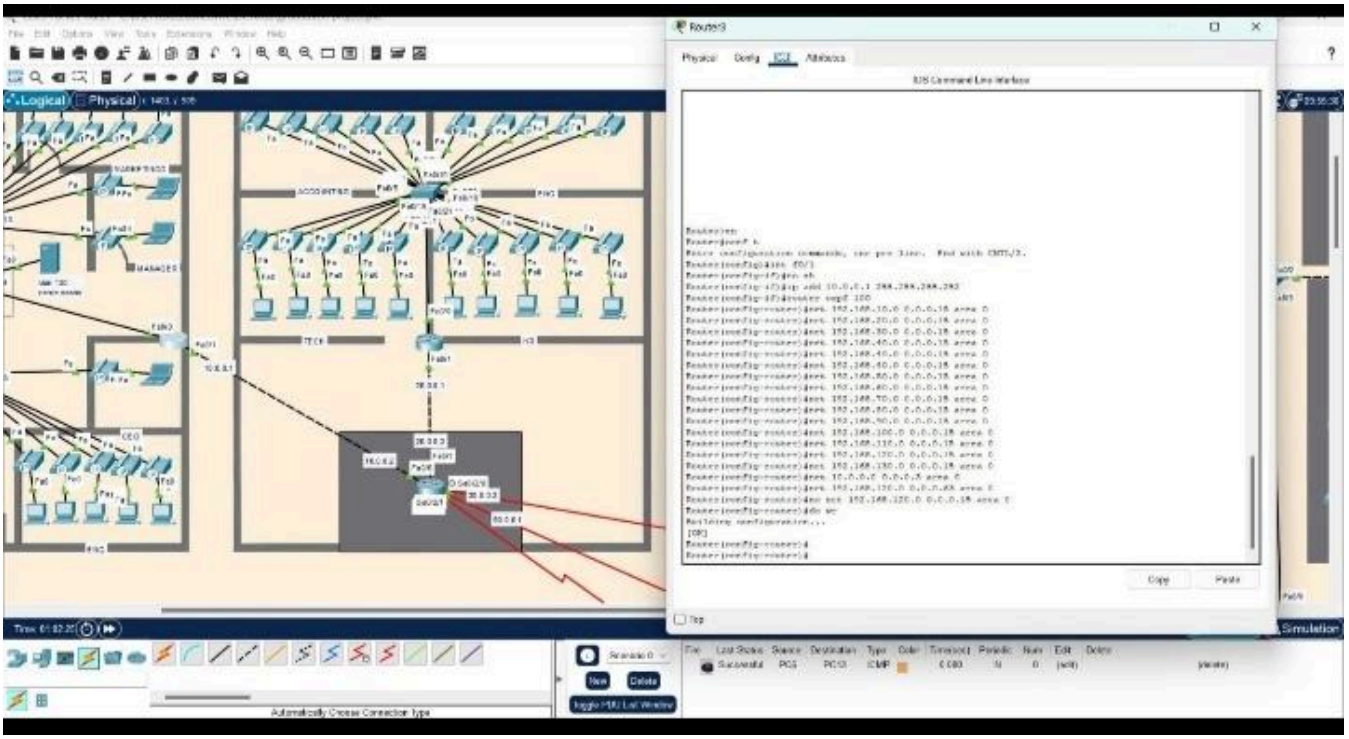


CamScanner


Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Realtime
Simulation
Automatically Choose Connection Type

CamScanner





CamScanner

Branch 3:Data center &Doc Office

this branch is logically and physically segmented across three switches (core sw,sw1,sw2)to support the following infrastructure:

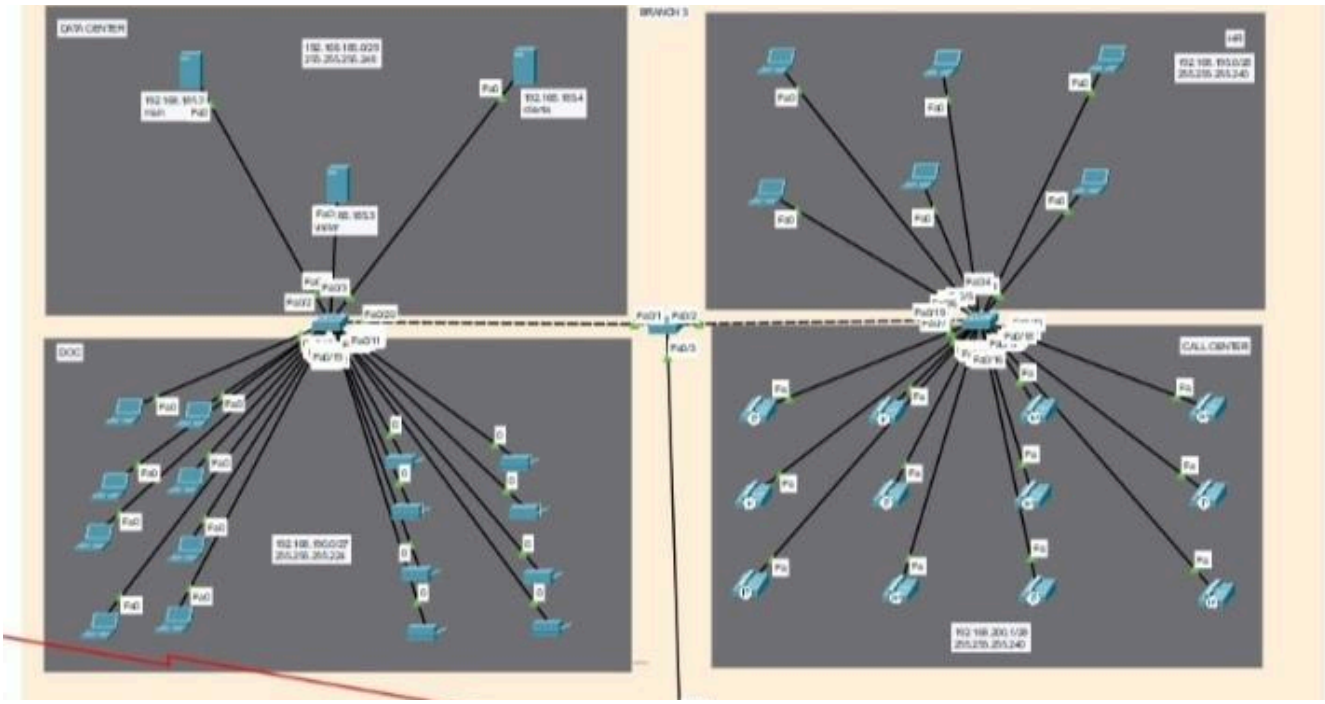
1-Data center Vlan 185

ports f0\1-3 on the first switch are dedicated to ensuring server isolation.A tightly controlled subnet 192.168.185.0/29 with the subnet mask 255.255.255.248 has been deployed to provide maximum protection and minimize the attack surface available to adversaries.

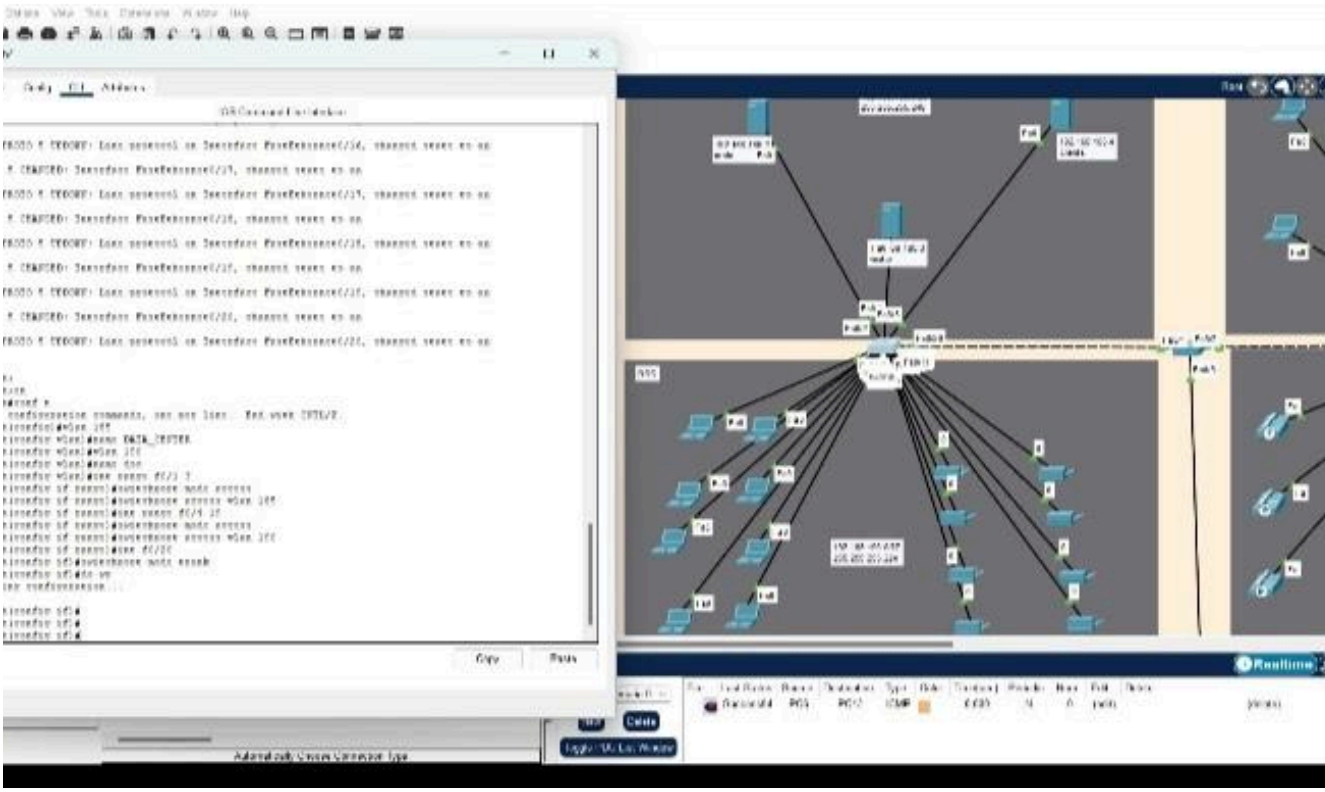
2-Document and Records Management(Vlan 190-Doc)

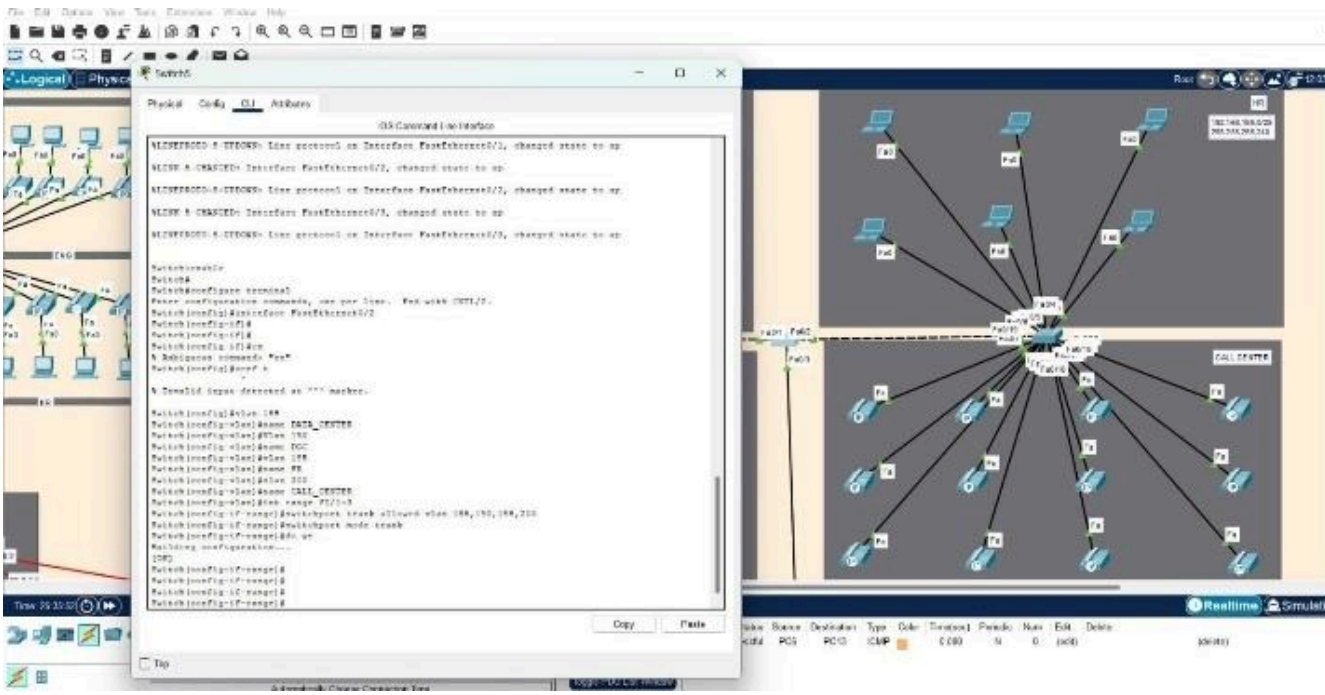
3-Administrative Department &connectivity(Vlan 195-HR and call center-Vlan 200)

the floor is equipped with voice over ip (voip)capabilities by assigning voice channels to Vlan 200,along with configuring the router's internal telephony service to support 12 ip phones with an extension range from 301 to 312.

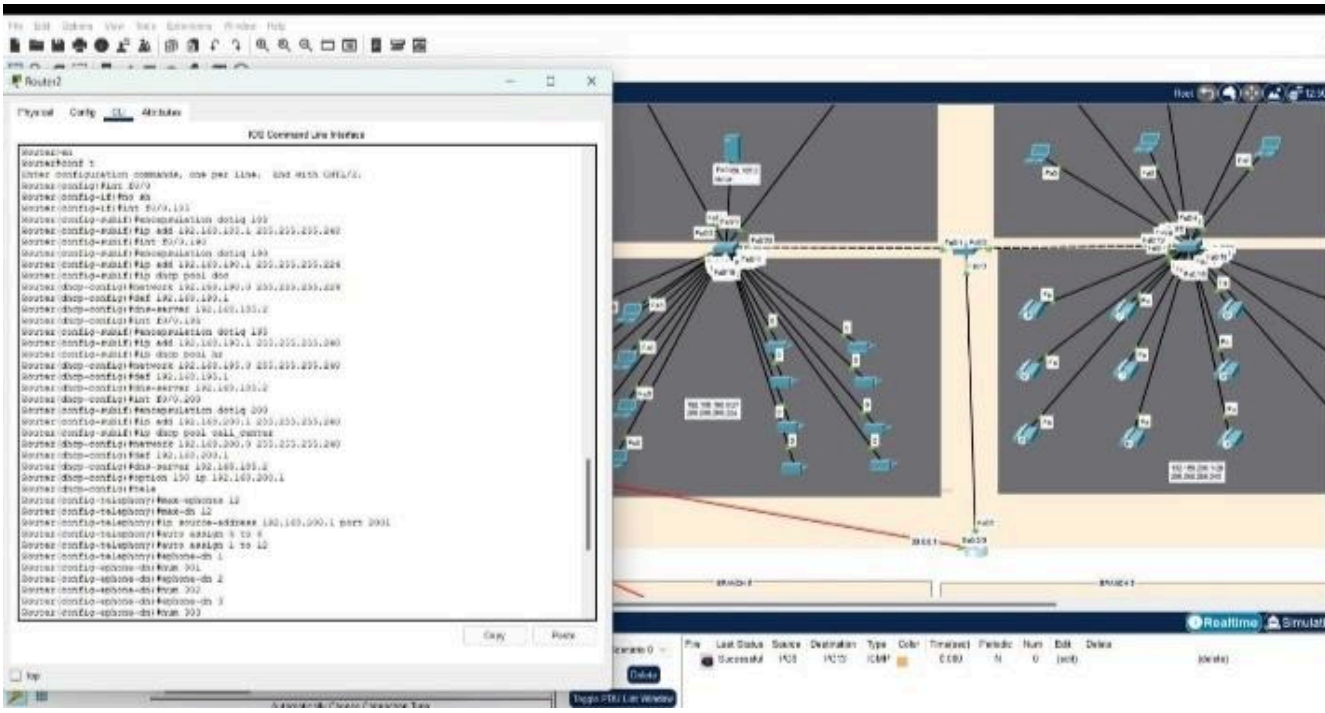


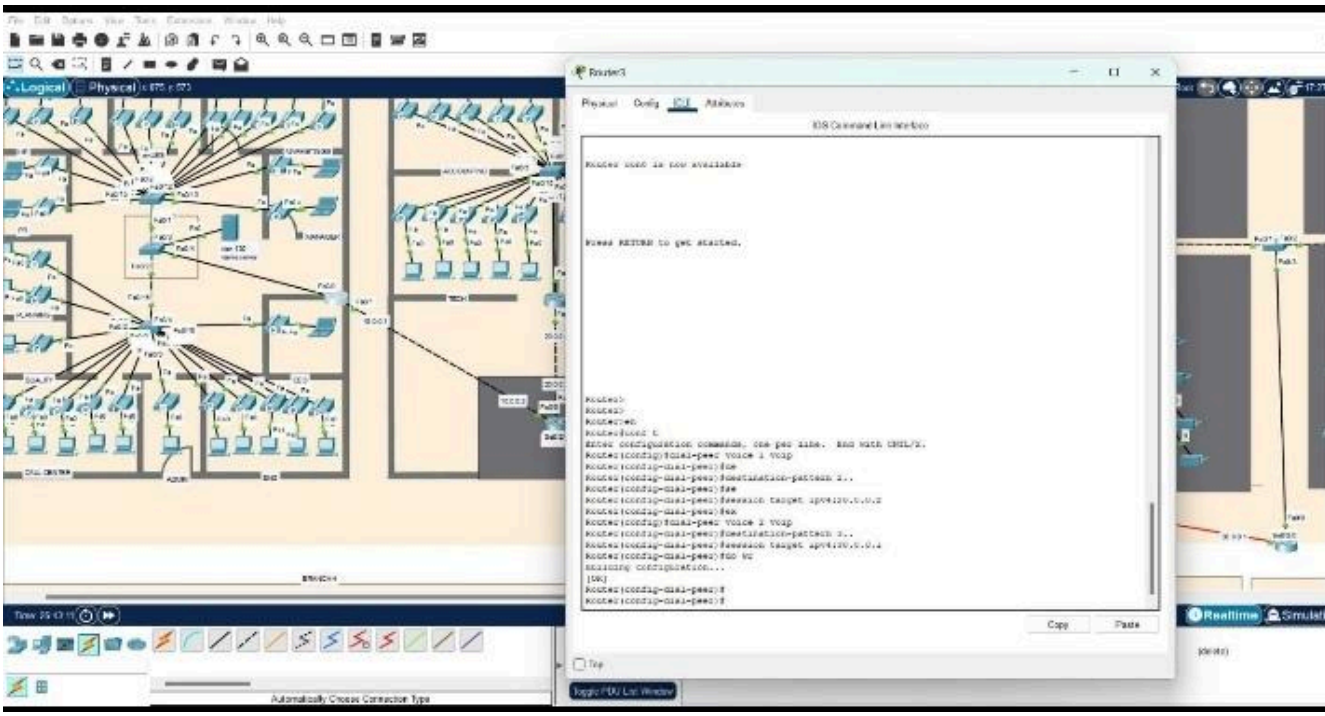
CamScanner



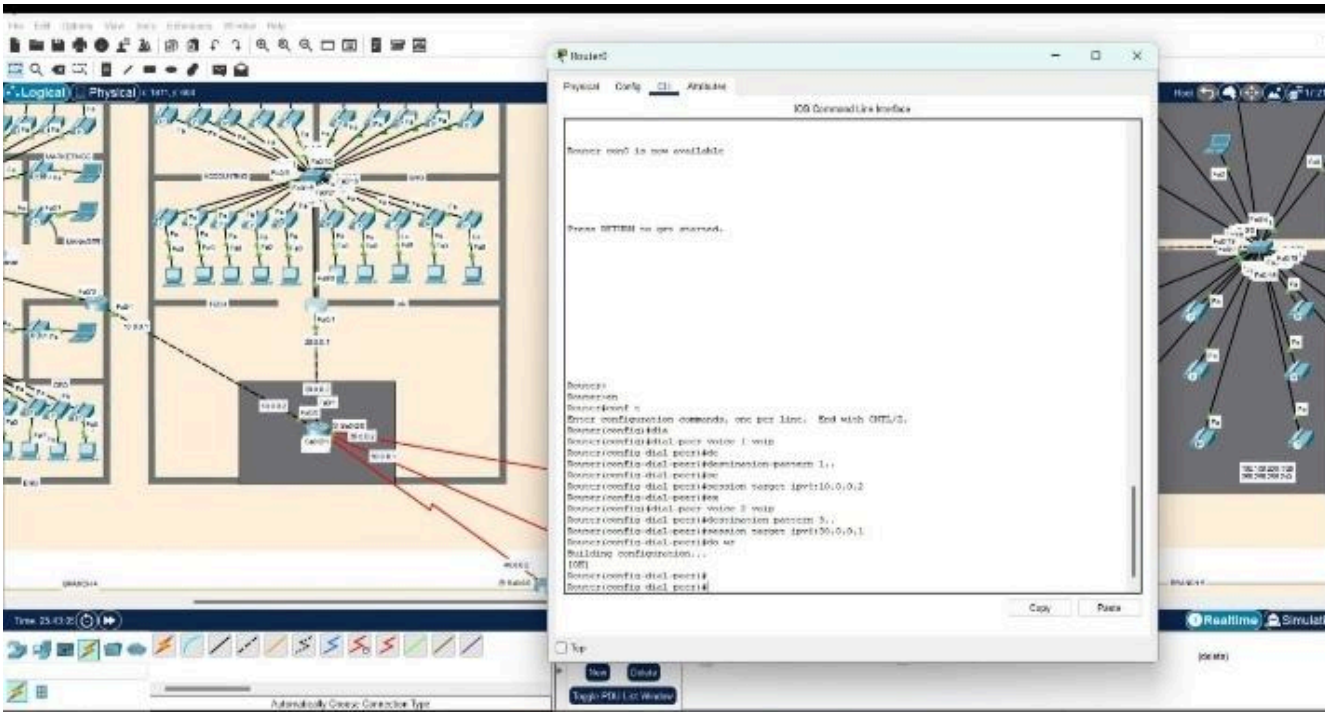


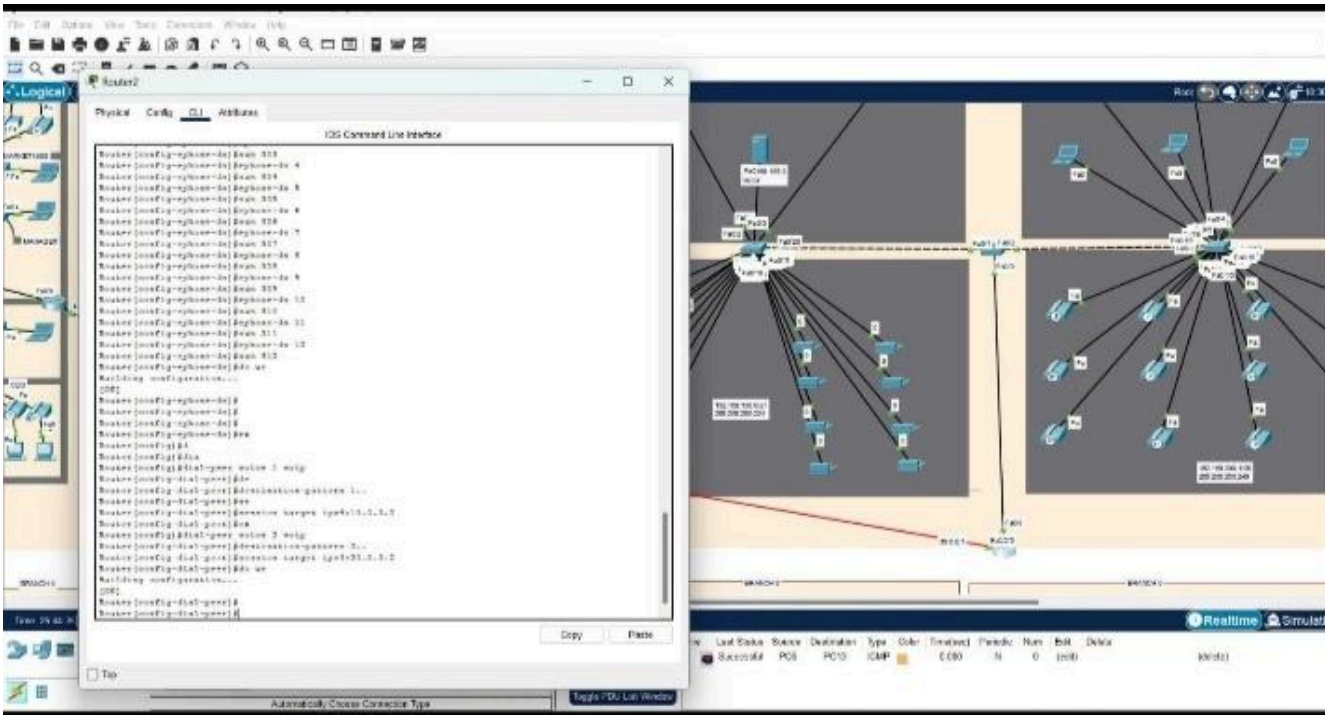
CamScanner



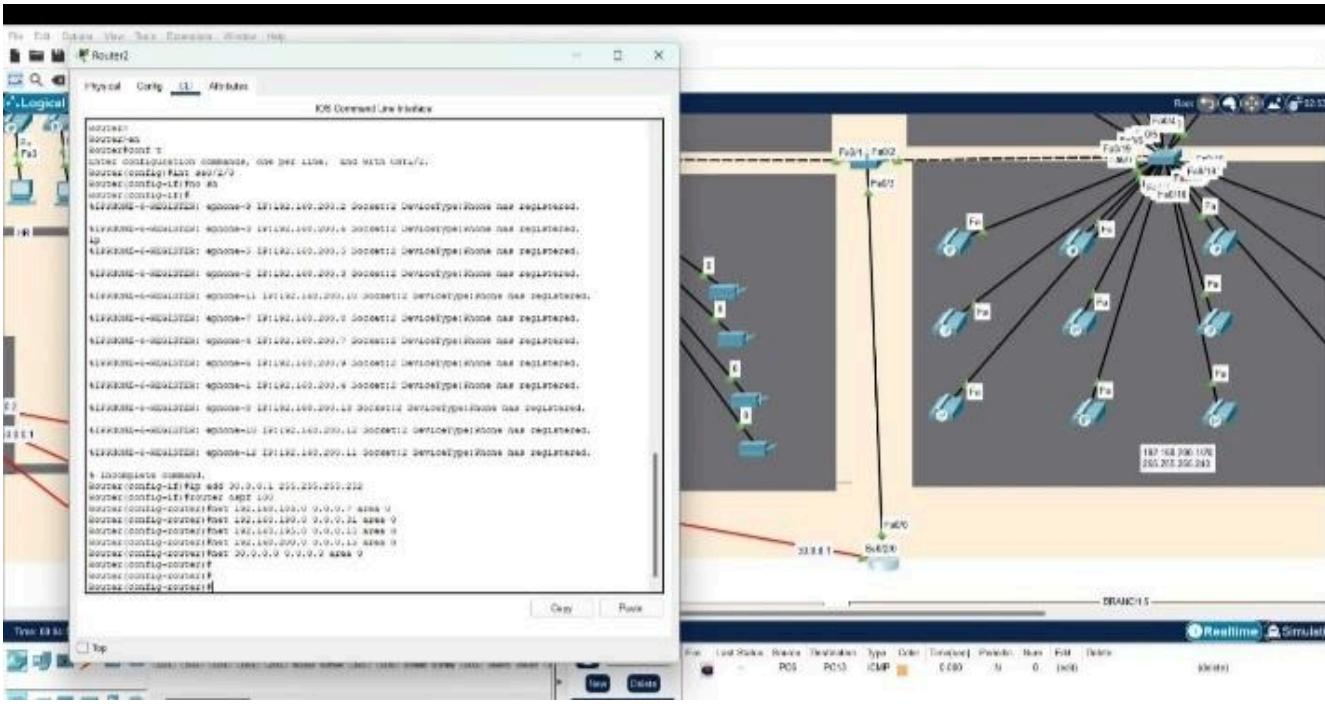


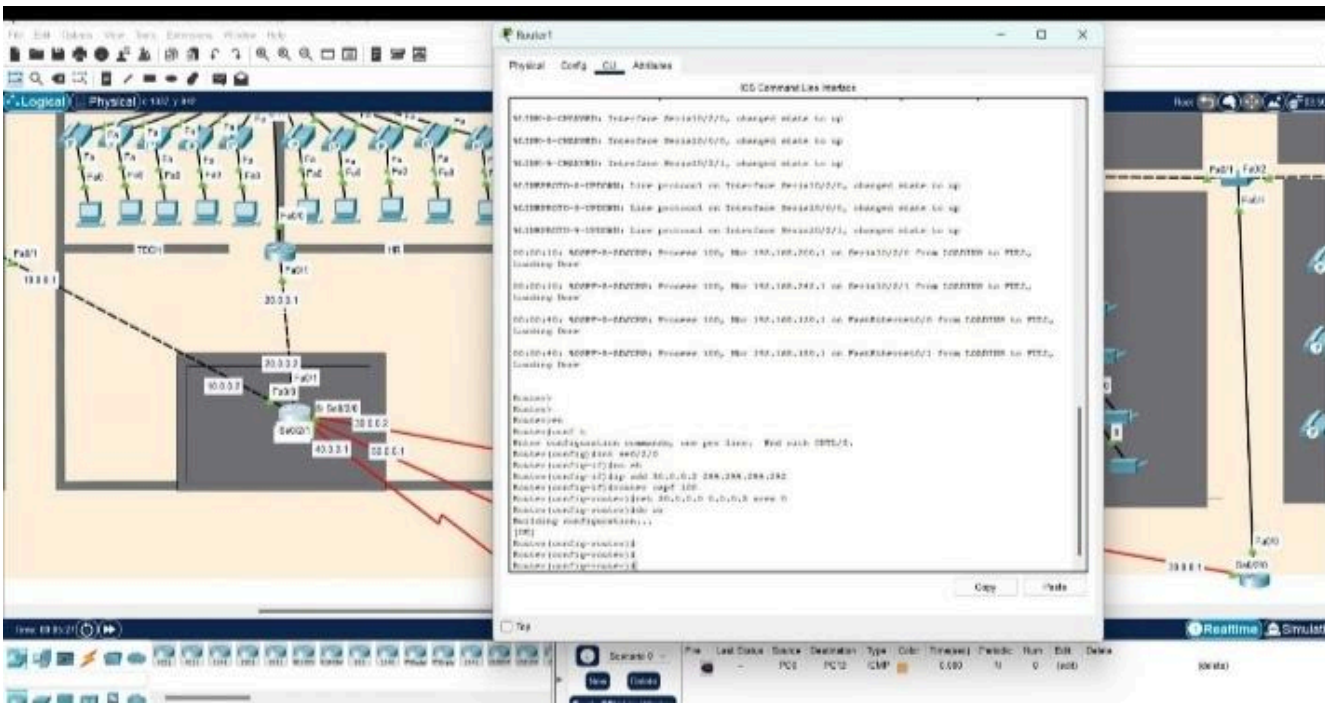
CamScanner





CamScanner





CamScanner

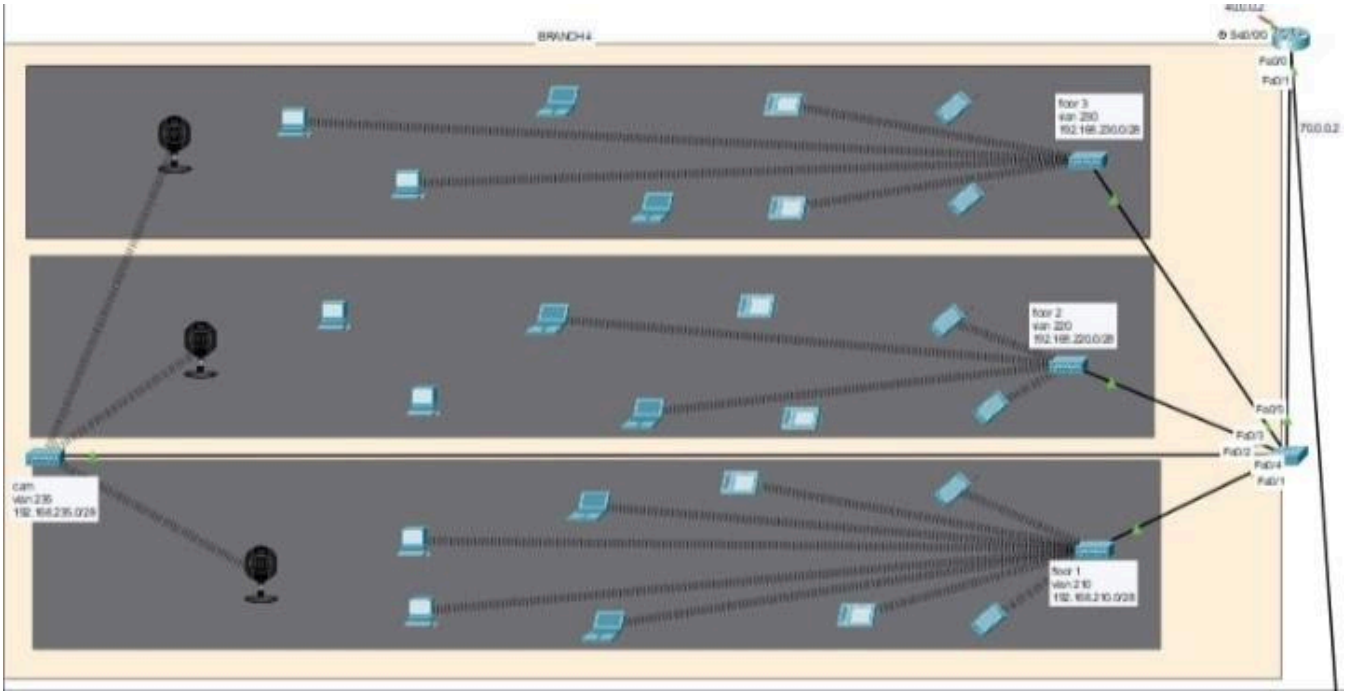
Branch 4:smart offices & surveillance camera system

is built as a fully wireless network environment .

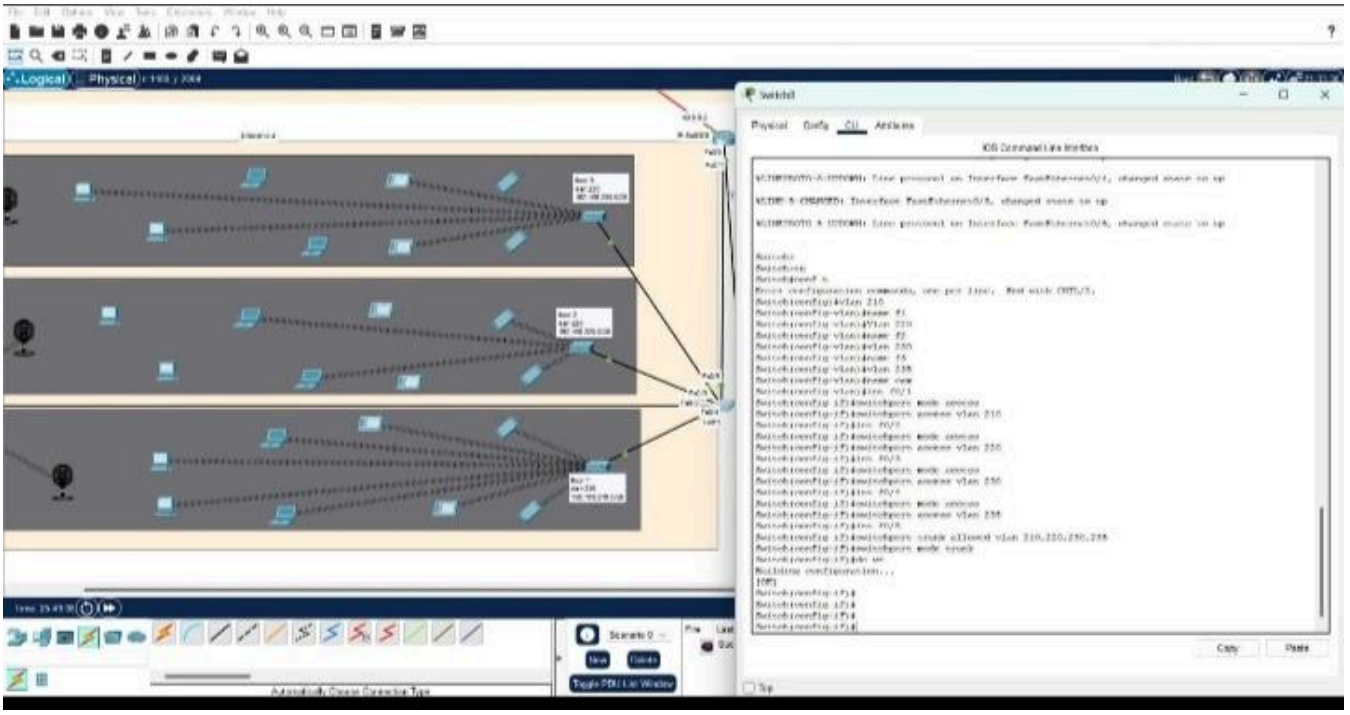
Vlans segmentation:

-floor networks (Vlan 210,220,230):Data traffic has been isolated for each floor individually (floor 1,floor 2,floor 3)

-surveillance network (Vlan 235-CAM)



CamScanner



CamScanner

Branch 5 end 6

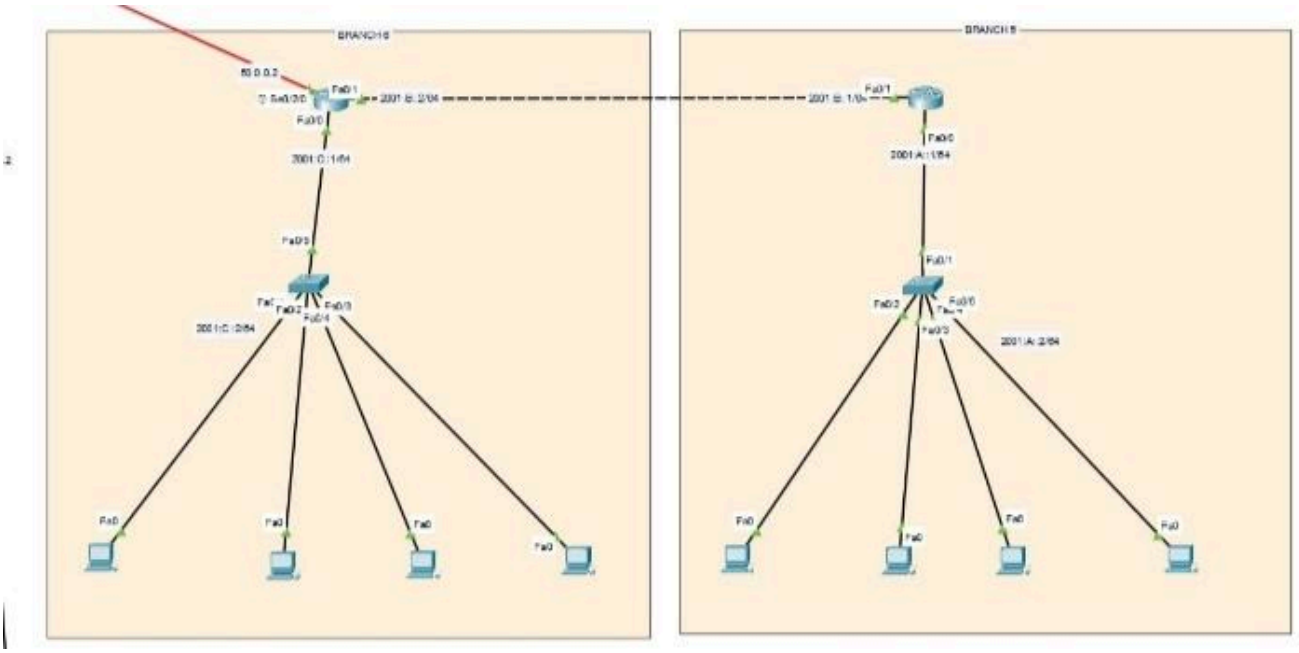
in these specific branches ,a transition from IPV4 to IPV6

Deploying IPV6 in these subnets fulfills the following objective

-Massive Address space:utilizing 128 bit addressing provides virtually unlimited ip subnet.

-Elimination of NAT:Every host in branch 5 and 6 obtains a globally unique ipv6 address

in these branches we used a multi- layered switching architecture to segment local departments into (Vlans)



CamScanner

Branch 7 and 8(branch lan &Routing configuration)

for the local area network (lan)design of both branch 7 and 8,traditional core routers were replaced with Multilayer Switches (L3 switches).This design choice provides several technical advantages:

-functionality integration:

- The device operates at layer 2 for high speed intra-Vlan switching ,while simultaneously operating at layer 3 to route traffic between different networks.

-Reduced complexity and hardware:

- The Multilayer switch acts as a central DHCP pools for each Vlan allocating ip addresses dynamically without requiring an external server .

Logical network segmentation (VLANs&Subneting)

Branch	Department	Vlan ID	Network subnet	Default gateway
branch 7	HR	241	192.168.241.0/28	192.168.241.1
branch 7	SALES	242	192.168.242.0/28	192.168.242.1
branch 8	MARKETING	243	192.168.243.0/28	192.168.243.1
branch 8	PLANNING	244	192.168.244.0/28	192.168.244.1

to establish connectivity between the branches and ensure seamless data transmission across the enterprise network, the following configuration steps were implemented:

1-configuring routed ports

BY applying the no switchport command on the physical interfaces of the multilayer switch,the ports were convert into routed ports . this allowed the assignment of direct ip addresses to connect with external routers and branch.

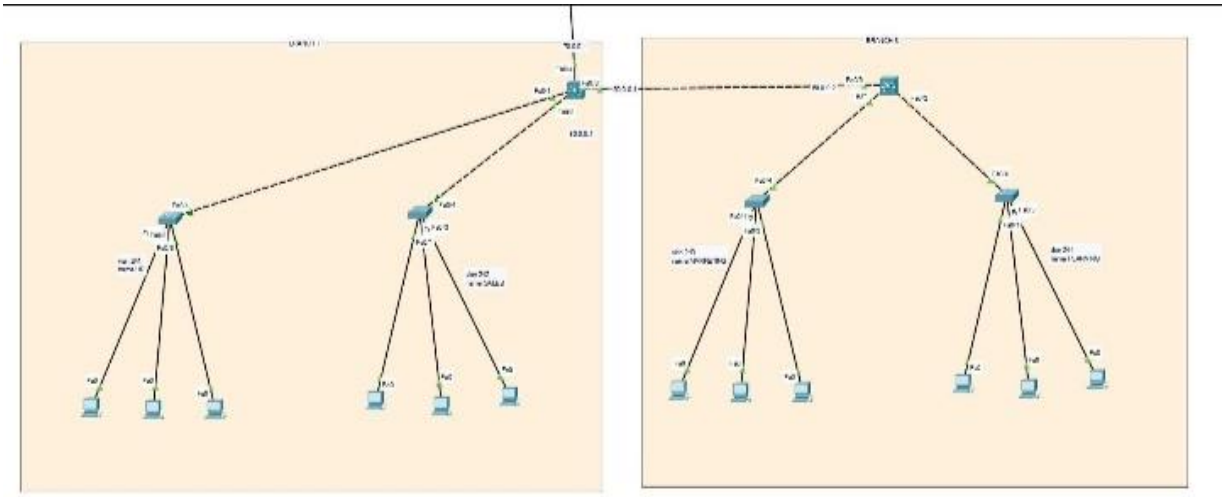
2-Enabling ip routing

CamScanner

in the multilayer switch to activate its routing table functionality

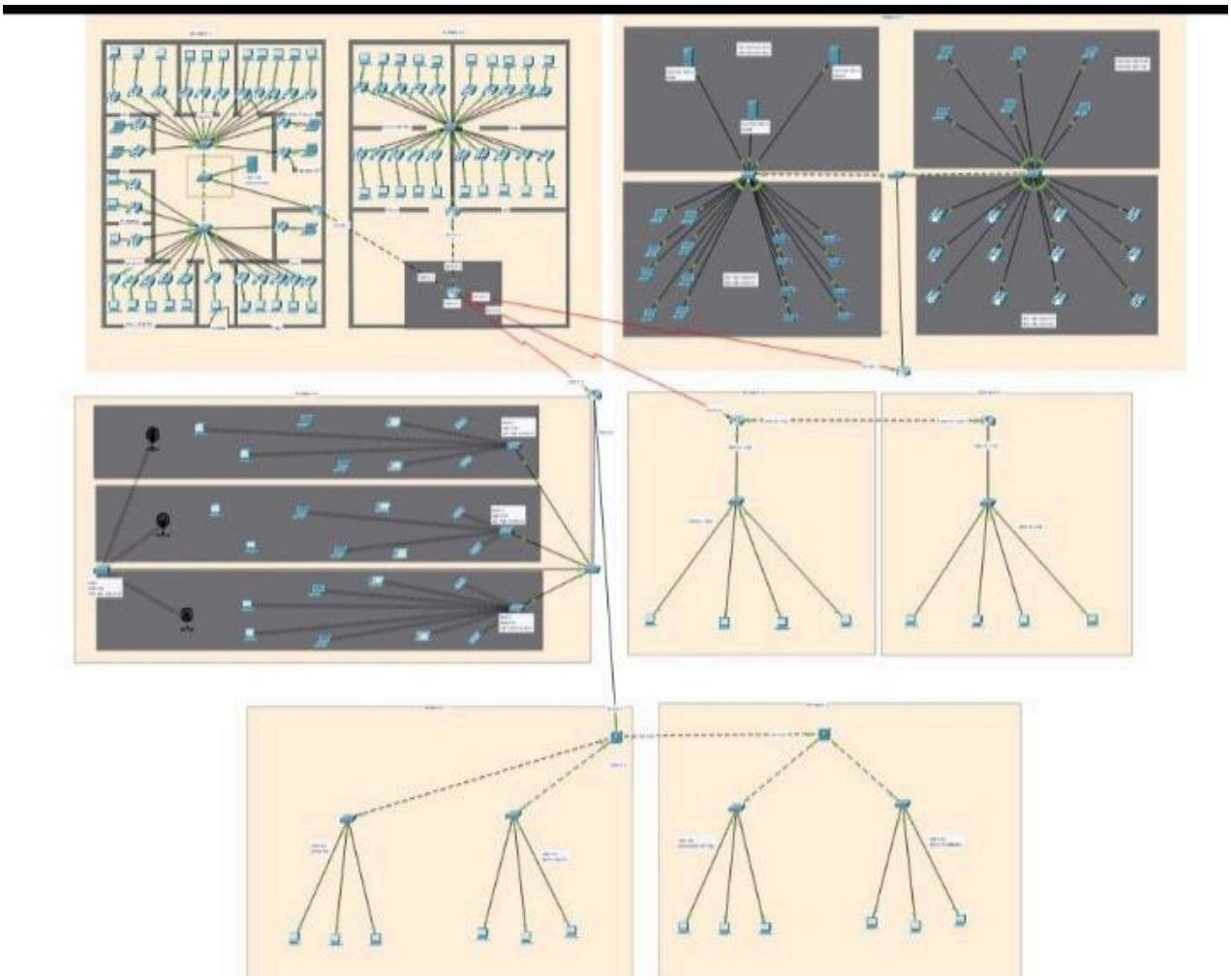
3-ospf Dynamic Routing protocol

ospf Area 0 was configured to advertise internal point to point link.



CamScanner

the total project



CamScanner

CONCLUSION

This work reflects a deep understanding of networking concepts and their practical application. It also enhances our technical abilities in network design and real-world troubleshooting.moreover,it demonstrates the value of combining simulation with physical implementation in professional network projects.

We hope this project serves as a technical reference and a stepping stone for more advanced future projects.

Acknowledgment:

We would like to express our sincere gratitude to professor :Ahmed Zakzouk and professor : Ragab El-Sagher for his continuous guidance,encouragement,and valuable feedback throughout the project. We also extend our thanks to all our team members for this cooperation ,dedication,and great team spirit.

References

1. Cisco. (n.d.). Voice over IP (VoIP). Cisco. Retrieved from https://www.cisco.com/c/en/us/solutions/collaboration/what-is-voip.html Last accessed on Feb 2.2025

2. GeeksforGeeks. (2021). OSI Model – 7 Layers Explained. Retrieved from https://www.geeksforgeeks.org/layers-of-osi-model/ last accessed on March 3,2025

3. TutorialsPoint. (n.d.). TCP/IP Model in Computer Networks. Retrieved from https://www.tutorialspoint.com/data_communication_computer_network/tcp_ip_model.htm last accessed on May 5,2025

4. NetworkLessons.com. (n.d.). OSPF (Open Shortest Path First). Retrieved from https://networklessons.com/cisco/ccna-routing-switching/ospf-openshortest

CamScanner